โครงการจ้างที่ปรึกษา
การพัฒนาระบบรักษาความมั่นคงความปลอดภัยด้านไซเบอร์ (Cybersecurity) ตามแผนขับเคลื่อน Smart Grid

สำนักงานนโยบายและแผนพลังงาน

๒๕๖๔

บทสรุปผู้บริหาร (Executive Summary)

ภาคส่วนไฟฟ้าถือเป็นหน่วยงานที่เป็นโครงสร้างพื้นฐานที่สำคัญของประเทศ (Critical Infrastructure: CI) ที่ต้องจัดหาพลังงานไฟฟ้าเพื่อรองรับความต้องการด้านการใช้พลังงานไฟฟ้าจำนวนมากในแต่ละวัน ผู้ประกอบกิจการไฟฟ้าจึงมีความจำเป็นต้องปกป้องระบบไฟฟ้าให้มีเสถียรภาพและพร้อมให้บริการอยู่เสมอ และปัจจุบันภาคไฟฟ้าได้มีการนำเทคโนโลยีสารสนเทศและการสื่อสารมาใช้ เพื่อให้การทำงานของระบบไฟฟ้าเป็นไปอย่างมีประสิทธิภาพและเพิ่มความน่าเชื่อถือ (Reliability) เพื่อขับเคลื่อนการไฟฟ้าสู่ยุคดิจิตอล (Digital Utility) ระบบ ICT ได้ถูกนำมาใช้งานมากขึ้นโดยเฉพาะในส่วนของการควบคุมและสั่งการ การผลิตไฟฟ้า (Generation) การส่งไฟฟ้า (Transmission) การจำหน่ายไฟฟ้า (Distribution) ไปจนถึงภาคการใช้ไฟฟ้า (Customer Premise) แต่ด้วยระบบเทคโนโลยีสารสนเทศ และการสื่อสาร (Information Technology and Communication: ICT) ได้มีการพัฒนาก้าวหน้าไปอย่างมาก อีกทั้งแนวโน้มของเทคโนโลยีและการสื่อสารที่เปลี่ยนแปลงไป ภัยคุกคามทางไซเบอร์ได้กลายเป็นภัยคุกคามที่ภาคส่วนพลังงานต้องคำนึงถึงและให้ความสนใจมากขึ้น เนื่องจากสามารถก่อให้เกิดเหตุการณ์ไฟฟ้าดับเป็นวงกว้างซึ่งจะส่งผลกระทบระดับประเทศได้

ความสำคัญและความจำเป็นในการปกป้องและหรือป้องกันด้านระบบไฟฟ้าจากภัยคุกคามไซเบอร์

ปัจจุบันเทคโนโลยีสารสนเทศและการสื่อสาร (Information Technology and Communication: ICT) ได้มีการพัฒนาก้าวหน้าไปอย่างมาก คอมพิวเตอร์มีความสามารถในการประมวลผลได้อย่างถูกต้องแม่นยำและรวดเร็วมากขึ้น ระบบเครือข่ายคอมพิวเตอร์ (Computer Networks) กลายเป็นโครงสร้างพื้นฐานสำคัญของการสื่อสารรับส่งข้อมูลได้ทั้งในระยะใกล้และไกล ซึ่งภาคส่วนต่าง ๆ ได้มีการนำเทคโนโลยีสารสนเทศมาใช้มากขึ้นอย่างกว้างขวาง สำหรับภาคไฟฟ้า ได้มีการนำเทคโนโลยีสารสนเทศและการสื่อสารมาใช้มากขึ้นโดยเฉพาะในส่วนของการควบคุมและสั่งการ การผลิตไฟฟ้า การส่ง การจำหน่ายไฟฟ้า ไปจนถึงในด้านการใช้ไฟฟ้า รวมถึงได้มีการขยายการเชื่อมต่อทางไซเบอร์กับเครือข่ายสื่อสารขององค์ประกอบต่าง ๆ ในระบบ เพื่อยกระดับการให้บริการเพื่อให้ตอบสนองต่อความต้องการของผู้ใช้ไฟฟ้าที่เพิ่มมากขึ้นได้อย่างรวดเร็ว รวมถึงเพื่อให้การไฟฟ้าสามารถบริหารจัดการระบบไฟฟ้าได้อย่างสะดวกและมีประสิทธิภาพมากขึ้น

การโจมตีทางไซเบอร์ทั่วโลกมีจำนวนเพิ่มมากขึ้นและมีความซับซ้อนเพิ่มมากขึ้นจากในอดีตที่ผ่านมา ยกตัวอย่างเช่น ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ระบบการควบคุมอุตสาหกรรมประเทศสหรัฐอเมริกา (ICS-CERT) ที่ได้เผยว่าภาคพลังงานเริ่มกลายเป็นเป้าหมายของการโจมตีทางไซเบอร์มากขึ้น โดยในปี ค.ศ. 2015 (พ.ศ. 2558) มีการรายงานว่าเกิดการโจมตีทางไซเบอร์ต่อระบบควบคุมและสั่งการการผลิตในประเทศสหรัฐอเมริกาจำนวน 295 ครั้ง โดย 46 ครั้งเป็นการโจมตีต่อภาคพลังงานโดยเฉพาะ

ด้วยระบบไฟฟ้ามีความสำคัญและกระทบต่อหลายภาคส่วน การรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) ให้กับระบบไฟฟ้าจึงเป็นประเด็นซึ่งมีความจำเป็นที่จะต้องดำเนินการ โดยนิยามของการรักษาความมั่นคงปลอดภัยทางไซเบอร์มีดังต่อไปนี้

นิยามของการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)[1]

การป้องกันความเสียหาย การปกป้อง และการฟื้นคืนสภาพของคอมพิวเตอร์ ระบบสื่อสารทางอิเล็กทรอนิกส์ การให้บริการการสื่อสารทางอิเล็กทรอนิกส์ การสื่อสารผ่านสายสัญญาณ และการสื่อสารทางอิเล็กทรอนิกส์ทั่วไป ซึ่งรวมถึงข้อมูลที่ถูกส่งผ่านไปมาด้วย เพื่อรักษาไว้ซึ่งความพร้อมใช้งาน (Availability) ความถูกต้องครบถ้วน (Integrity) การรับรอง (Authentication) การรักษาความลับ (Confidentiality) และการปฏิเสธไม่ได้ (Non-repudiation)

ระบบเทคโนโลยีสารสนเทศและการสื่อสารที่เกี่ยวข้องกับระบบไฟฟ้าในประเทศไทย

ระบบไฟฟ้าเป็นโครงสร้างพื้นฐานที่มีความสำคัญสูง (Critical Infrastructure: CI) ปัจจุบัน ได้เริ่มมีการนำระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information and Communication Technology: ICT) เข้ามาเป็นองค์ประกอบในการดำเนินงานมากขึ้นในภาคไฟฟ้าตามความก้าวหน้าของเทคโนโลยี โดยมีทั้งส่วนที่นำไปใช้ในระบบควบคุมและสั่งการการปฏิบัติการระบบไฟฟ้า การเชื่อมโยงข้อมูลระยะทางไกลผ่านเครือข่ายความเร็วสูง นอกจากนี้ เทคโนโลยีสมาร์ทกริดได้ถูกนำเข้ามาใช้งานมากขึ้นเพื่อช่วยให้การบริหารจัดการระบบไฟฟ้าให้มีความชาญฉลาดมากขึ้น ทำให้ใช้งานระบบได้อย่างเต็มประสิทธิภาพ ซึ่งเทคโนโลยีสมาร์ทกริดทำงานได้อย่างอัตโนมัติบนพื้นฐานของเทคโนโลยี ICT เป็นหลัก

ในผลการศึกษาฉบับนี้ จะศึกษาถึงสถานการณ์ระบบไฟฟ้าในประเทศไทยโดยแบ่งออกเป็นสองหัวข้อหลักได้แก่

- **ระบบไฟฟ้าปัจจุบัน (พ.ศ. 2563-2564)** รวมถึงองค์ประกอบของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่เกี่ยวข้องกับระบบไฟฟ้า[2]
- **ระบบไฟฟ้าของประเทศไทยในอนาคตภายใต้การดำเนินงานด้านสมาร์ทกริด (พ.ศ. 2565 ขึ้นไป)** รวมถึงองค์ประกอบของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่เกี่ยวข้องกับระบบไฟฟ้า[3]โดยจัดกลุ่มการศึกษาตามเสาหลักในการดำเนินการด้านสมาร์ทกริดของประเทศไทยทั้งหมด 3 เสาหลัก ประกอบด้วย
  - เสาหลักที่ 1 การตอบสนองด้านโหลดและระบบบริหารจัดการพลังงาน
  - เสาหลักที่ 2 ระบบพยากรณ์ไฟฟ้าที่ผลิตได้จากพลังงานหมุนเวียน
  - เสาหลักที่ 3 ระบบไมโครกริดและระบบกักเก็บพลังงาน

[1] ที่มา: https://csrc.nist.gov/glossary/term/cybersecurity (ต้นฉบับนิยามภาษาอังกฤษ: Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.)

[2] บทที่ 3 ระบบเทคโนโลยีสารสนเทศและการสื่อสารที่เกี่ยวข้องกับระบบไฟฟ้าในประเทศไทย (หัวข้อ 3.1)

[3] บทที่ 3 ระบบเทคโนโลยีสารสนเทศและการสื่อสารที่เกี่ยวข้องกับระบบไฟฟ้าในประเทศไทย (หัวข้อ 3.2)

รูปที่ EX-1 ขอบเขตการศึกษาระบบ ICT ของระบบไฟฟ้าประเทศไทย

จากการวิเคราะห์ผลการศึกษาของข้อมูลระบบ ICT ที่เกี่ยวข้องกับระบบไฟฟ้าในปัจจุบัน และแนวโน้มการปรับเปลี่ยนระบบเทคโนโลยีสารสนเทศและการสื่อสารในอนาคตของการไฟฟ้าฝ่ายผลิตแห่งประเทศไทย (กฟผ.) การไฟฟ้าส่วนภูมิภาค (กฟภ.) และการไฟฟ้านครหลวง (กฟน.) พบว่าได้มีการนำเทคโนโลยีเข้ามาใช้งานในงานที่สำคัญต่าง ๆ ได้แก่

- **ระบบสารสนเทศของศูนย์ควบคุมและสั่งการ** หน่วยงานการไฟฟ้าทั้ง 3 แห่ง มีระบบงานหลักเดียวกัน ได้แก่ ระบบ Supervisory Control And Data Acquisition (SCADA) เพื่อควบคุมสั่งการจ่ายไฟอัตโนมัติ ระบบ Energy Management System (EMS) เพื่อบริหารจัดการพลังงานไฟฟ้าในระบบ (ซึ่งสำหรับ กฟภ. และ กฟน. จะเป็น Distribution Management System (DMS) เพื่อบริหารจัดการการจ่ายไฟฟ้าในระบบจำหน่าย)
- **โครงสร้างระบบเครือข่ายและการสื่อสาร** หน่วยงานการไฟฟ้าทั้ง 3 แห่ง ได้มีการติดตั้งระบบโครงข่ายใยแก้วนำแสงหลัก (Backbone Fiber Optic) เพื่อใช้สำหรับการเชื่อมต่อระหว่างศูนย์ควบคุมและสั่งการกับโรงไฟฟ้า หรือสถานีย่อยของหน่วยงาน โดยใช้โปรโตคอลสื่อสารที่สามารถทำงานบนโปรโตคอล IP ได้ เช่น DNP3 over IP หรือ ICCP over IP
- **การพัฒนาระบบสมาร์ทกริด** หน่วยงานการไฟฟ้าทั้ง 3 แห่ง ได้มีการพัฒนาโครงการด้านระบบสมาร์ทกริดอย่างต่อเนื่อง และยังคงมีความสอดคล้องกับแผนแม่บทการพัฒนาระบบโครงข่ายสมาร์ทกริดของ ประเทศไทย พ.ศ. 2558-2579 รวมถึงการปรับปรุงโครงสร้างระบบ ICT เพื่อให้รองรับกับเทคโนโลยีสมาร์ทกริดในอนาคต โดยกลุ่มของระบบสมาร์ทกริดที่คาดการณ์ว่าจะมีการพัฒนาระบบนำร่อง รวมถึงขยายผลไปใช้ในงานบริการประชาชนในช่วง 5 ปีนี้ (พ.ศ.2563 – 2567) ได้แก่ ระบบ

มิเตอร์ไฟฟ้าอัจฉริยะ (Smart Meter) ระบบบริหารจัดการข้อมูลมิเตอร์ (Meter Data Management System: MDMS) ระบบไมโครกริด (Microgrid) ระบบกักเก็บพลังงาน (Energy Storage System: ESS) ระบบการตอบสนองด้านโหลด (Demand Response: DR) ระบบบริหารจัดการด้านโหลด (Demand-Side Management: DSM) เป็นต้น โดยแนวโน้มการพัฒนาเทคโนโลยีตามแผนแม่บทสมาร์ทกริดของประเทศไทยของ กฟผ. จะแสดงในรูปที่ EX-2 และของ กฟภ. และ กฟน. จะแสดงในรูปที่ EX-3 ตามลำดับ

EGAT

Smart grid & ICT Technology	1 - 5 ปี	5-10 ปี	10 ปีขึ้นไป
Demand Response (DR)	→		
Renewable Energy Forecast System	→		
Microgrid/Energy Storage System	→		
ETC	-	-	-

รูปที่ EX-2 แนวโน้มการพัฒนาระบบสมาร์ทกริดของ กฟผ.

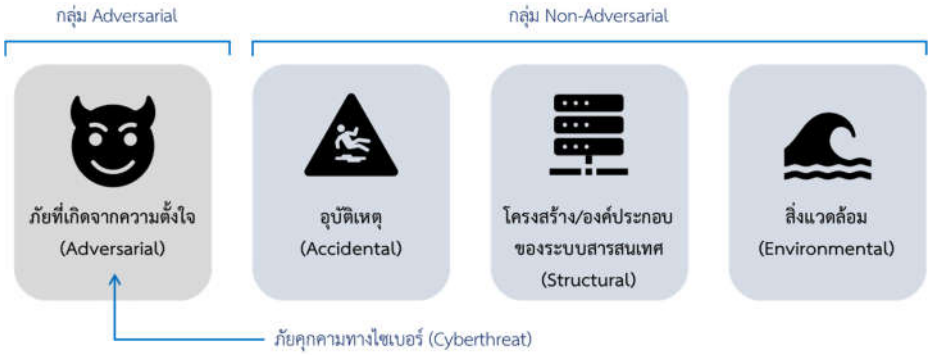
PEA / MEA

Smart grid & ICT Technology	1 - 5 ปี	5-10 ปี	10 ปีขึ้นไป
Distribution/Feeder Automation (DA/FA)	→	→	→
Substation Automation	→	→	→
Distribution Management System (SCADA/DMS)	→	→	→
Smart Meter + AMR/AMI	→	→	→
Intelligent Charging System/V2G	-	→	→
Demand Response (DR)/Demand-Side Management (DSM)	→	→	→
Intelligent Street Lights	-	-	-
Meter Data Management System	→	→	→
Microgrid Development	→	→	→
Energy Storage System	→	→	→
SPP/VSPP Data Communication System	→	→	→
Virtual Power Plant	→	→	→
ETC	-	-	-

รูปที่ EX-3 แนวโน้มการพัฒนาระบบสมาร์ทกริดของ กฟภ. และ กฟน.

ประเภทของภัยคุกคามทางไซเบอร์ที่อาจจะเกิดขึ้นต่อด้านระบบไฟฟ้า

เหตุขัดข้องต่าง ๆ ที่อาจส่งผลกระทบต่อระบบไฟฟ้า เกิดได้จากหลายสาเหตุ โดยแบ่งภัยคุกคามทางไซเบอร์ออกเป็น 2 ประเภท[4] ได้แก่ (1) **Non-Adversarial Threat** เช่น ภัยคุกคามที่เกิดขึ้นโดยธรรมชาติ เช่น แผ่นดินไหว อุทกภัย หรือเกิดจากการกระทำโดยไม่ตั้งใจ หรือความผิดพลาดของตัวระบบ และ (2) **Adversarial Threat** ได้แก่ ภัยคุกคามที่เกิดจากผู้กระทำมีความตั้งใจหรือมีแรงจูงใจในการคุกคามหรือทำความเสียหาย หรือทำอันตรายต่อระบบไฟฟ้า (ดังปรากฏในรูปที่ EX-4) อย่างไรก็ตาม ผลกระทบที่เกิดกับระบบไฟฟ้าไม่ว่าจากภัยคุกคามประเภทใด ก็อาจส่งผลกระทบต่อระบบไฟฟ้าโดยรวมทั้งประเทศได้ เช่น ระบบไฟฟ้าขาดแคลนกำลังผลิตไฟฟ้าเป็นจำนวนมาก หรืออาจก่อให้เกิดการเกิดเหตุการณ์ไฟฟ้าดับในวงกว้าง ซึ่งจะส่งผลกระทบต่อผู้ใช้ไฟฟ้าตามครัวเรือน และอุตสาหกรรมต่าง ๆ ภัยคุกคามทางไซเบอร์จัดอยู่ในกลุ่ม Adversarial Threat



รูปที่ EX-4 ประเภทของภัยคุกคาม

จากสถิติพบว่าภัยคุกคามทางไซเบอร์ที่มีแนวโน้มเพิ่มจำนวนมากขึ้นในปัจจุบัน พบว่ากลุ่มที่สามารถสร้างความเสียหายต่อระบบไฟฟ้าได้สูงจะเกิดจาก Adversarial Threat หรือกลุ่มผู้โจมตีที่มีแรงจูงใจอย่างใดอย่างหนึ่ง ไม่ว่าจะเป็นสาเหตุทางการเมือง ความมั่นคงของชาติ หรือเพื่อแสวงหาผลประโยชน์ทางการเงิน หรือเพียงสร้างความสนุกสนาน ผู้โจมตีกลุ่มนี้ได้พัฒนาทักษะและความชำนาญของตนเองสูงขึ้นอย่างสม่ำเสมอ มีการสร้างเครื่องมือในการโจมตี เช่น มัลแวร์ประเภทใหม่ ๆ ที่มีความซับซ้อนและออกแบบมาโดยเฉพาะรวมถึงสามารถหลบซ่อนการตรวจจับจากเทคโนโลยีต่าง ๆ ในปัจจุบันได้ เช่น Advanced Persistent Threats (APT) ไม่ว่าจะเป็น STUXNET, Havex, BlackEnergy หรือ Industroyer ซึ่งพบว่าได้มีการใช้เทคนิคนี้ในการโจมตีระบบไฟฟ้าได้สำเร็จ และก่อให้เกิดความเสียหายต่อระบบไฟฟ้าของประเทศแล้วจริง เช่น กรณีเหตุการณ์การโจมตีไซเบอร์ต่อระบบไฟฟ้าในประเทศยูเครน ในปี พ.ศ. 2558 (ค.ศ. 2015) และ พ.ศ. 2559 (ค.ศ. 2016) ส่งผลให้ไฟฟ้าดับในวงกว้างเป็นเวลานาน กระทบต่อประชากรจำนวนมาก

จากผลการศึกษาพบว่าภาคส่วนไฟฟ้าได้มีจุดอ่อนหรือช่องโหว่ที่ผู้ไม่ประสงค์ดีนำมาใช้เพื่อโจมตีการทำงานของระบบได้โดยง่าย ประกอบด้วย การขาดความตระหนักด้านความมั่นคงปลอดภัยของผู้ปฏิบัติงาน

[4] อ้างอิงตามมาตรฐาน NIST 800-30 Guide for Conducting Risk Assessments

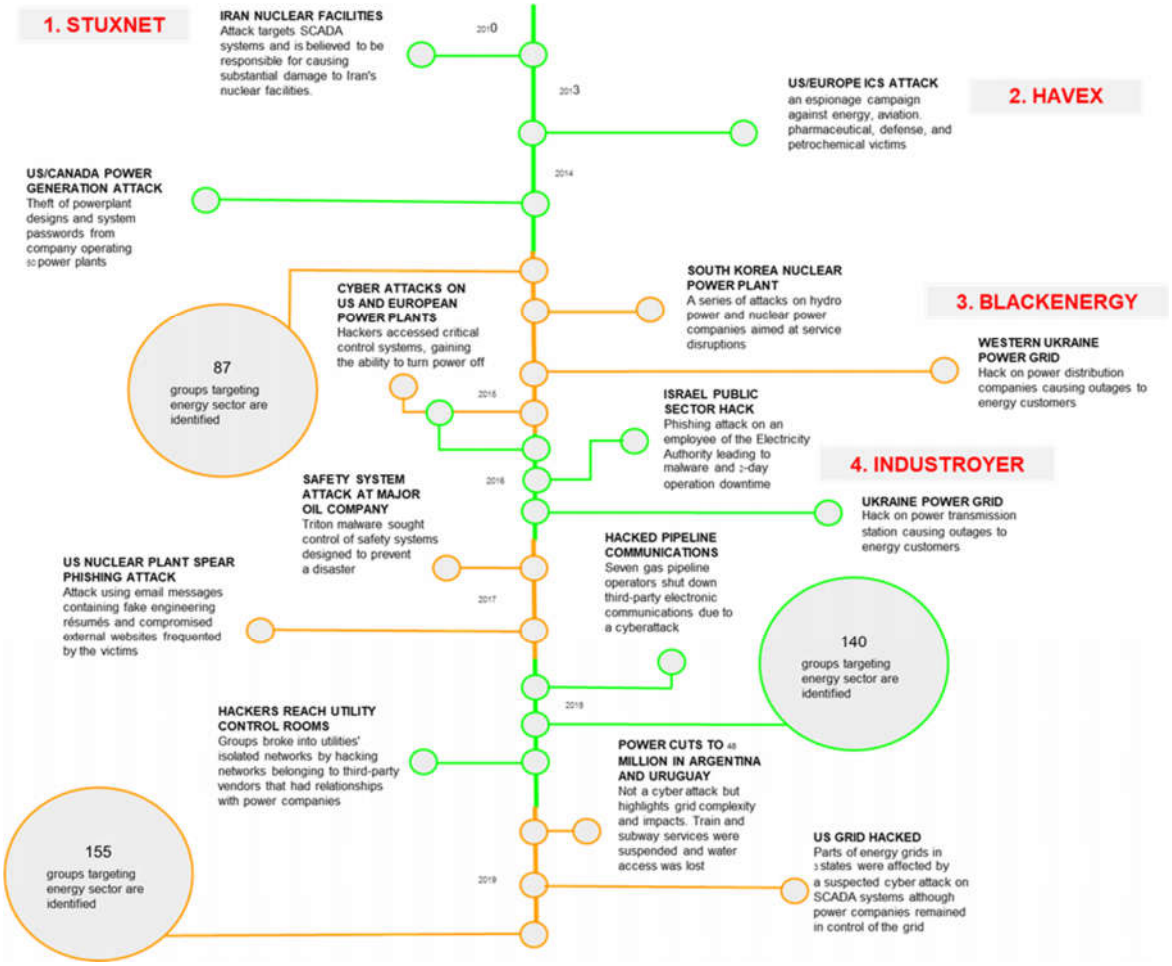
การขาดการควบคุมทางเทคนิค ทั้งด้านการป้องกัน การเฝ้าระวัง หรือการตรวจจับสิ่งผิดปกติหรือมัลแวร์ต่าง ๆ การใช้งานระบบปฏิบัติการที่ล้าสมัยและมีช่องโหว่ การใช้งาน Removable media กับระบบที่ต้องการความมั่นคงปลอดภัย จุดอ่อนหรือช่องโหว่เหล่านี้ จำเป็นต้องได้รับการตรวจสอบและกำหนดแนวทางในการป้องกันและรักษาความมั่นคงปลอดภัยไซเบอร์ของระบบไฟฟ้าอย่างเหมาะสม

หน่วยงานที่เกี่ยวข้องในภาคส่วนไฟฟ้าทั้งจากภาครัฐและเอกชน จำเป็นต้องมีความตระหนักรู้ ติดตามสถานการณ์และแนวโน้มด้านความมั่นคงปลอดภัยอย่างต่อเนื่อง รวมถึงประเมินความเสี่ยงที่อาจเกิดขึ้นจากเหตุการณ์ภัยคุกคามไซเบอร์อยู่เสมอ เพื่อปกป้องระบบไฟฟ้าจากภัยคุกคามดังกล่าวและควบคุมไม่ให้เกิดความสูญเสียทางด้านการเงิน เศรษฐกิจ ความมั่นคงของประเทศ ความปลอดภัยในชีวิตและทรัพย์สิน และความสงบสุขของประชาชน

กรณีศึกษา รูปแบบภัยคุกคามทางไซเบอร์ต่อระบบไฟฟ้าที่เกิดขึ้นในต่างประเทศ

การพิจารณาภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับระบบไฟฟ้าของไทย ได้มีการศึกษาและเรียนรู้ถึงวิธีการโจมตีทางไซเบอร์ที่เคยเกิดขึ้นในต่างประเทศมาแล้ว ดังปรากฏในบทที่ 1[5] เพื่อให้ทราบถึงตัวอย่างเหตุการณ์และความรุนแรงของผลกระทบที่เกิดในอดีต และทราบถึงลักษณะของการโจมตี ช่องทางหรือช่องโหว่ที่เสี่ยงต่อการโดนโจมตี รวมถึงผลกระทบที่เกิดขึ้นต่อระบบไฟฟ้า เป็นข้อมูลตั้งต้นสำหรับการกำหนดแนวทางและมาตรการในการป้องกันและรับมือภัยคุกคามไซเบอร์เหล่านั้นที่อาจเกิดขึ้นได้ในอนาคต ซึ่งได้สรุปกรณีศึกษาภัยคุกคามทางไซเบอร์ต่อระบบไฟฟ้าที่เกิดขึ้นในต่างประเทศ ได้แก่ Stuxnet, Havex, BlackEnergy และ Industroyer ดังปรากฏในรูปที่ EX-5 และ ตารางที่ EX-1

[5] บทที่ 1 ผลการศึกษาข้อมูลภัยคุกคามทางไซเบอร์ด้านระบบไฟฟ้า มาตรการปกป้องและ/หรือป้องกันระบบไฟฟ้าในต่างประเทศ



รูปที่ EX-5 สถานการณ์ภัยคุกคามทางไซเบอร์ต่อระบบไฟฟ้าทั่วโลก

ตารางที่ EX- 1 สรุปกรณีศึกษาภัยคุกคามทางไซเบอร์ต่อระบบไฟฟ้าที่เกิดขึ้นในต่างประเทศ

ชื่อ	เป้าหมาย	ประเภทภัยคุกคาม	มูลเหตุจูงใจ	ผลกระทบ
Stuxnet	ประเทศอิหร่าน	Nation-state	การเมือง	อาจเกิดผลกระทบทางกายภาพโดยการเร่งให้ใบพัดของเตาปฏิกรณ์โรงไฟฟ้านิวเคลียร์หมุนเร็วขึ้นจนเกิดความร้อนและเกิดการระเบิด
Havex	ยุโรปและประเทศสหรัฐอเมริกา	ไม่สามารถระบุได้	ไม่สามารถระบุได้ หมายเหตุ : แม้จะไม่ได้เป็นการสร้างความเสียหายต่อเป้าหมาย แต่ข้อมูลที่ถูกขโมยออกไปอาจถูกนำไปใช้ในการโจมตีครั้งต่อไป	ข้อมูลรั่วไหล
BlackEnergy	ประเทศยูเครน	Nation-state หรือ Hacker	การเมือง	ไฟฟ้าดับในวงกว้าง
Industroyer	ประเทศยูเครน	Nation-state	การเมือง	ไฟฟ้าดับในวงกว้าง

แนวทางการศึกษาและตัวอย่างการประเมินความเสี่ยงต่อระบบไฟฟ้าจากภัยคุกคามทางไซเบอร์

การประเมินความเสี่ยงต่อระบบไฟฟ้าจากภัยคุกคามทางไซเบอร์ จำเป็นต้องมีหลักการในการพิจารณาวิธีการบริหารจัดการความเสี่ยงให้เหมาะสมต่อการดำเนินงาน โดยจากการศึกษามาตรฐานสากลพบว่ามาตรฐานการประเมินความเสี่ยงซึ่งเป็นที่นิยมใช้กันอย่างกว้างขวาง ประกอบด้วย NIST 800-3, ISO/IEC27005 และ ISO 31000 โดยมีแนวทางนำไปประยุกต์ใช้งาน ดังปรากฏในตารางที่ EX-2

ตารางที่ EX-2 สรุปภาพรวมของตัวอย่างมาตรฐานการประเมินความเสี่ยงในต่างประเทศ

มาตรฐาน	ปัจจัยการประเมิน	ระดับความเสี่ยง	การนำไปใช้งาน
NIST 800-3 Guide for Conducting Risk Assessments	● โอกาสที่จะเกิดเหตุการณ์ (Likelihood) – 5 ระดับ ● ผลกระทบ (Impact) – 5 ระดับ (แบ่งพิจารณาออกเป็น 5 ด้าน)	5 ระดับ	การประเมินความเสี่ยงในรายละเอียดของการนำเทคโนโลยีสารสนเทศมาใช้ในการขับเคลื่อนธุรกิจขององค์กร
ISO/IEC27005 – Information Technology — Security techniques — Information security risk management	● โอกาสที่จะเกิดเหตุการณ์ (Likelihood) – 5 ระดับ ● ผลกระทบทางธุรกิจ (Business Impact) – 5 ระดับ	5 ระดับ	การประเมินความเสี่ยงในรายละเอียดของการนำเทคโนโลยีสารสนเทศมาใช้ในการขับเคลื่อนธุรกิจขององค์กร
ISO 31000 Risk management – Guidelines	-	-	การบริหารจัดการความเสี่ยงในภาพใหญ่ระดับองค์กร

โดยทั่วไปแล้ว หลักการการประเมินความเสี่ยงของมาตรฐานที่กล่าวมาในข้างต้นจะคล้ายคลึงและเป็นไปในแนวทางเดียวกัน (ดังปรากฏในรูปที่ EX-6) ประกอบด้วย

(1) การกำหนดขอบเขตในการประเมินระดับความเสี่ยง โดยพิจารณาได้จากภารกิจของหน่วยงาน ขอบเขตการให้บริการ กระบวนการทางธุรกิจและทรัพย์สินทางไซเบอร์ที่เกี่ยวข้องกับกระบวนการเหล่านั้น เพื่อให้สามารถระบุประเมินถึงเหตุการณ์การคุกคามทางไซเบอร์ที่อาจเกิดขึ้นต่อทรัพย์สินเหล่านั้นได้

(2) ดำเนินการพิจารณาระดับความเสี่ยง โดยเริ่มจากการระบุถึงเหตุการณ์การคุกคามทางไซเบอร์ที่เป็นไปได้ เพื่อนำมาประเมินความเสี่ยง โดยพิจารณาจากประเภทของภัยคุกคามประกอบกับแนวทางที่

ผู้ไม่ประสงค์ดีใช้ในการคุกคามต่อทรัพย์สินทางไซเบอร์ที่อยู่ภายในขอบเขตที่พิจารณาตามข้อ (1) จากนั้นจึงประเมินความเป็นไปได้ (Likelihood) และผลกระทบ (Impact) ที่อาจเกิดขึ้นต่อทรัพย์สินทางไซเบอร์นั้น รวมถึงผลกระทบต่อส่วนอื่นที่อาจเกิดขึ้นได้หากทรัพย์สินทางไซเบอร์เกิดความเสียหาย ทั้งนี้ ไม่มีมาตรฐานใดที่กำหนดหลักเกณฑ์การประเมินความเป็นไปได้ (Likelihood) และผลกระทบ (Impact) โดยละเอียด ดังนั้น หน่วยงานที่ประเมินความเสี่ยงจะต้องเป็นผู้พิจารณากำหนดเกณฑ์ให้เหมาะสมกับบริบทของตนเอง

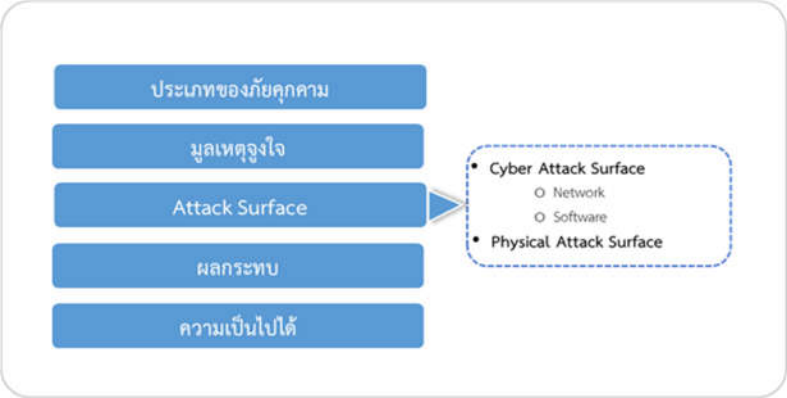
(3) พิจารณาดำเนินการรับมือต่อความเสี่ยง หลังจากเมื่อองค์กรได้ทราบถึงระดับความเสี่ยงแล้วจึงพิจารณาหาแนวทางในการรับมือกับความเสี่ยงเหล่านั้น

รูปที่ EX-6 ขั้นตอนหลักในการประเมินความเสี่ยงด้านไซเบอร์

การวิเคราะห์ความเสี่ยงของภัยคุกคามทางไซเบอร์ต่อระบบไฟฟ้า

จากการศึกษาระบบเทคโนโลยีสารสนเทศและการสื่อสารที่เกี่ยวข้องกับระบบไฟฟ้า และแนวทางการศึกษาและตัวอย่างการประเมินความเสี่ยงต่อระบบไฟฟ้าจากภัยคุกคามทางไซเบอร์ข้างต้น ได้นำผลการศึกษามาดำเนินการพิจารณาถึงความเสี่ยงที่จะเกิดขึ้นกับระบบไฟฟ้าของประเทศโดยการศึกษาและประเมินระดับความเสี่ยงของภัยคุกคามไซเบอร์ในภาคไฟฟ้าของไทยจะวิเคราะห์ภายในขอบเขตที่ครอบคลุมถึง ระบบไฟฟ้าของประเทศไทยในปัจจุบัน และระบบไฟฟ้าของประเทศไทยในอนาคตภายใต้การดำเนินงานด้านสมาร์ทกริด โดยมีกรอบการประเมินความเสี่ยง ดังปรากฏในรูปที่ EX-7[6]

[6] บทที่ 4 ผลการศึกษาและประเมินระดับความเสี่ยงของภัยคุกคามทางไซเบอร์ต่อระบบไฟฟ้าของประเทศไทย



รูปที่ EX-7 กรอบการประเมินความเสี่ยงด้านไซเบอร์

การวิเคราะห์ Attack Surface ของระบบไฟฟ้าของประเทศไทย ซึ่งสามารถถูกคุกคามได้ทางไซเบอร์ และช่องทางอื่น ๆ

สถาบัน SANS[7] และสถาบัน ISC2[8] ได้นิยาม “Attack Surface” ไว้ในทิศทางเดียวกัน โดยหมายถึง ส่วนใดส่วนหนึ่งของระบบที่อาจเป็นช่องทางที่ผู้ไม่ประสงค์ดีใช้ในการบุกรุกเข้าไปในระบบคอมพิวเตอร์ และอาจทำให้เกิดการเปิดเผย การเปลี่ยนแปลง หรือการทำลายข้อมูลโดยไม่ได้รับอนุญาต การจำกัด Attack surface ให้น้อยลงจะสามารถลดความเสี่ยงของการถูกโจมตีได้[9] Attack surface สามารถแบ่งออกได้เป็น 3 กลุ่ม ดังต่อไปนี้

- **Network Attack Surface**: ส่วนใดส่วนหนึ่งของระบบเครือข่ายที่อาจเป็นช่องทางที่ผู้ไม่ประสงค์ดีใช้ในการบุกรุกเข้าถึงระบบได้ โดยครอบคลุมถึงอุปกรณ์ (Devices) เช่น เราเตอร์ ไฟร์วอล เครื่องคอมพิวเตอร์พกพา สมาร์ทโฟน (Smart Phone) รวมถึง เฟิร์มแวร์ของอุปกรณ์ (Firmware) โปรโตคอล (Protocol) และพอร์ต (Port) ในการสื่อสารสำหรับให้บริการแอปพลิเคชันทางเครือข่าย (Services)
- **Software Attack Surface**: ส่วนใดส่วนหนึ่งของซอฟต์แวร์หรือองค์ประกอบในการทำงานของซอฟต์แวร์ รวมถึงส่วนที่เชื่อมต่อในการทำงานหรือรับส่งข้อมูล (Interface) ที่อาจเป็นช่องทางที่ผู้ไม่ประสงค์ดีใช้ในการบุกรุกเข้าถึงระบบได้
- **Human Attack Surface**: ช่องโหว่ที่เกิดจากกิจกรรม การดำเนินงาน หรือการตัดสินใจอย่างใดอย่างหนึ่งของบุคคล ไม่ว่าจะเป็นการละเลยในการปฏิบัติหน้าที่ การปฏิบัติงานหรือการตัดสินใจที่ผิดพลาด หรือการกระทำใด ๆ ที่อาจส่งผลต่อสุขภาพ อนามัย และชีวิต ซึ่งเกิดจากการกระทำโดยบุคลากรภายในองค์กร (Insider) ซึ่งกลุ่มนี้เป็นกลุ่มที่มีความเสี่ยงที่จะตกเป็นเป้าหมายของการโจมตีแบบ Social Engineering มากที่สุด

[7] องค์กรเพื่อความร่วมมือในการวิจัยและการศึกษาด้านการรักษาความปลอดภัยทางไซเบอร์

[8] สถาบันสำหรับจัดอบรมและให้การรับรองด้านความมั่นคงปลอดภัยของสหรัฐอเมริกา

[9] ที่มา : SANS: ICS Attack Surfaces ISC2, ICS LEXICON

สรุปตัวอย่าง Attack Surface ของระบบไฟฟ้าของประเทศไทย

ตารางที่ EX-3 ตัวอย่าง Attack Surface ของระบบไฟฟ้าของประเทศไทย

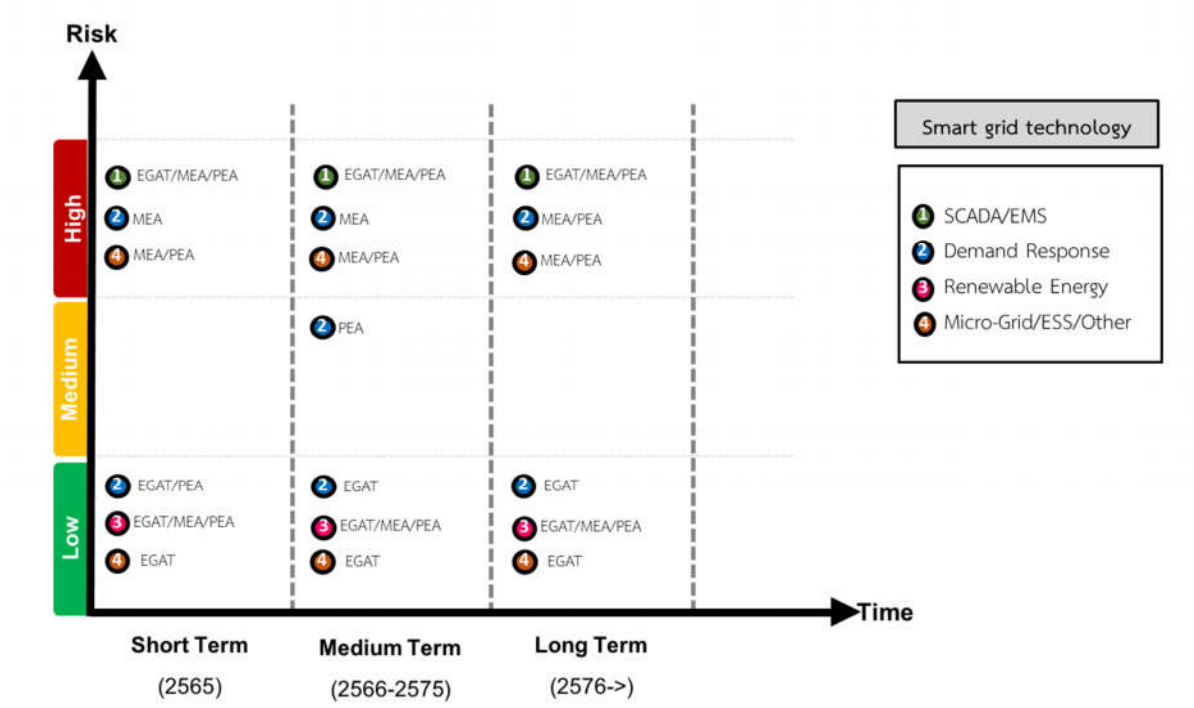
Attack surface	การผลิต/ส่ง/จำหน่ายไฟฟ้าไฟฟ้า	สมาร์ทกริด
การเข้าถึงข้อมูลของระบบไฟฟ้า		
Network Attack Surface (ครอบคลุมถึงอุปกรณ์และโปรโตคอล)	• การเชื่อมต่อระหว่างศูนย์ควบคุมและสั่งการ (Control Center) และเครือข่ายในโรงไฟฟ้า หรือสถานีไฟฟ้าย่อย ประเภท LAN หรือ WAN • โปรโตคอลที่ไม่เข้ารหัส • อุปกรณ์ภาคสนาม (Field Device) เช่น อุปกรณ์ตรวจวัด ฯลฯ	• โครงข่ายระบบมิเตอร์ไฟฟ้าอัจฉริยะ (Advanced metering infrastructure : AMI) • โครงข่ายระบบไมโครกริด • อุปกรณ์ Smart appliance
การเข้าถึงข้อมูลของระบบไฟฟ้าของประเทศไทยต่อโลกไซเบอร์ซึ่งครอบคลุมช่องทางอื่น ๆ ที่ไม่ใช่ระบบเครือข่ายคอมพิวเตอร์หรืออินเทอร์เน็ต		
Software Attack Surface	• ระบบ SCADA / ระบบ EMS /ระบบ DMS • ระบบบริหารจัดการกระแสไฟฟ้าขัดข้อง (Outage Management System: OMS)	• ระบบบริหารจัดการข้อมูลมิเตอร์ (Meter Data Management System: MDMS) • ระบบมิเตอร์ไฟฟ้าอัจฉริยะ (Advanced metering infrastructure: AMI) • ระบบ Demand Response
Human Attack Surface	• บุคลากรภายในองค์กร • ผู้ให้บริการภายนอก	• ผู้ใช้ไฟฟ้า

ผลวิเคราะห์ผลกระทบของภัยคุกคามทางไซเบอร์ที่มีต่อระบบไฟฟ้าของประเทศไทย

จากผลการศึกษาและประเมินระดับความเสี่ยงของภัยคุกคามทางไซเบอร์ต่อระบบไฟฟ้าของประเทศไทยในภาพรวมพบว่าระดับความเสี่ยงปัจจุบันยังคงอยู่ใน**ระดับต่ำ** เนื่องจาก Grid Cyber Asset ของระบบควบคุมและสั่งการระบบไฟฟ้า ยังคงเป็นระบบที่ไม่มีการเชื่อมต่อออกไปยังเครือข่ายสาธารณะโดยตรง และได้มีการกำหนดมาตรการควบคุมที่จำเป็น เช่น การเข้ารหัสช่องทางสื่อสาร เป็นต้น การไฟฟ้าต่าง ๆ ได้มีการควบคุมความเสี่ยงด้านความมั่นคงปลอดภัยที่เป็นมาตรฐาน ทำให้ความน่าจะเป็นหรือความเป็นไปได้ที่จะถูกคุกคามด้านไซเบอร์ยังคงอยู่ในระดับต่ำ แม้ว่าผลกระทบของภัยคุกคามทางไซเบอร์ที่มีต่อระบบไฟฟ้าอาจมีโอกาสเกิดได้สูงสุดด้วยสาเหตุของภัยคุกคามทางไซเบอร์ ได้แก่ เหตุการณ์ไฟฟ้าดับเป็นวงกว้าง เช่นเดียวกับภัยคุกคามด้านอื่น ๆ แต่ในอดีตที่ผ่านมา ยังไม่พบว่าเคยมีเหตุการณ์ที่ภัยคุกคามทางไซเบอร์ส่งผลกระทบระดับสูงต่อระบบไฟฟ้ามาก่อน อย่างไรก็ตาม ระดับความเสี่ยงของภัยคุกคามทางไซเบอร์ต่อระบบไฟฟ้าของประเทศไทยในอนาคตจะมีแนวโน้มที่สูงขึ้น เนื่องจาก

- ปัจจุบันพบว่ามีความพยายามโจมตีด้านไซเบอร์ในประเทศไทยอย่างต่อเนื่อง (Frequency)
- ภาคส่วนไฟฟ้ามีแนวโน้มที่จะตกเป็นเป้าหมายของการถูกคุกคามทางไซเบอร์เพิ่มและรุนแรงขึ้นอย่างต่อเนื่อง ปัจจุบันมีการโจมตีที่ก่อให้เกิดผลกระทบร้ายแรงเกิดขึ้นแล้วจริงในต่างประเทศ (Probability)
- Attack surface จะมีจำนวนเพิ่มมากขึ้น จากการนำเทคโนโลยี ICT มาใช้ รวมถึง Smart Cyber Asset ที่จะเข้ามาพร้อมกับการพัฒนาระบบสมาร์ทกริด โดยคาดว่าจะเริ่มมีการใช้งานที่ครอบคลุมมากขึ้นในระยะ 1-5 ปีขึ้นไปต่อจากนี้
- ภัยคุกคามรูปแบบใหม่ที่อาจเกิดขึ้นได้ในอนาคตสามารถสร้างผลกระทบระดับสูงในรูปแบบใหม่ต่อผู้ใช้ไฟฟ้า เช่น การพัฒนามัลแวร์ที่ใช้ในการเข้าถึงและควบคุมระบบของรถยนต์พลังงานไฟฟ้า (Electric Vehicle : EV) เป็นต้น

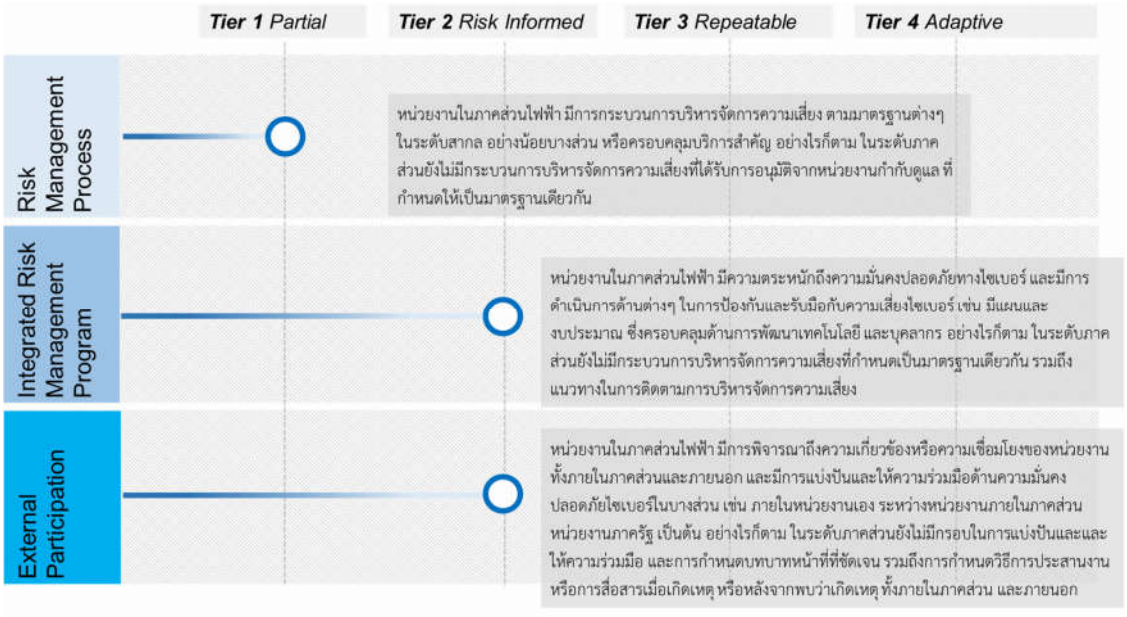
ผลการประเมินระดับความเสี่ยงของภัยคุกคามทางไซเบอร์ต่อระบบไฟฟ้าของประเทศไทยและแนวโน้มในอนาคตดังปรากฏในรูปที่ EX-8 จะเห็นได้ว่าในระยะยาวเทคโนโลยีดังกล่าวจะมีระดับความเสี่ยงต่อภัยคุกคามทางไซเบอร์สูง



รูปที่ EX-8 สรุปความเสี่ยงของภัยคุกคามทางไซเบอร์ต่อระบบไฟฟ้าของประเทศไทยในด้านต่าง ๆ

โดยจากผลการศึกษาในด้านการเตรียมความพร้อมเพื่อรับมือต่อความเสี่ยงด้านภัยคุกคามทางไซเบอร์ของภาคส่วนไฟฟ้าทั้งในปัจจุบันและอนาคตซึ่งพิจารณาจากระดับความพร้อมตามระดับ Implementation Tier ของ NIST Cybersecurity framework (CSF) พบว่าหน่วยงานในภาคไฟฟ้าควรต้องพิจารณาประเด็นต่าง ๆ ร่วมกัน เพื่อกำหนดแผนการดำเนินงานที่เหมาะสมต่อไป โดยในขั้นต่ำควรมีการดำเนินการเพื่อบริหารจัดการความเสี่ยงทางไซเบอร์อย่างเหมาะสม ดังปรากฏในรูปที่ EX-9[10]

[10] บทที่ 4 ผลการศึกษาและประเมินระดับความเสี่ยงของภัยคุกคามทางไซเบอร์ต่อระบบไฟฟ้าของประเทศไทย

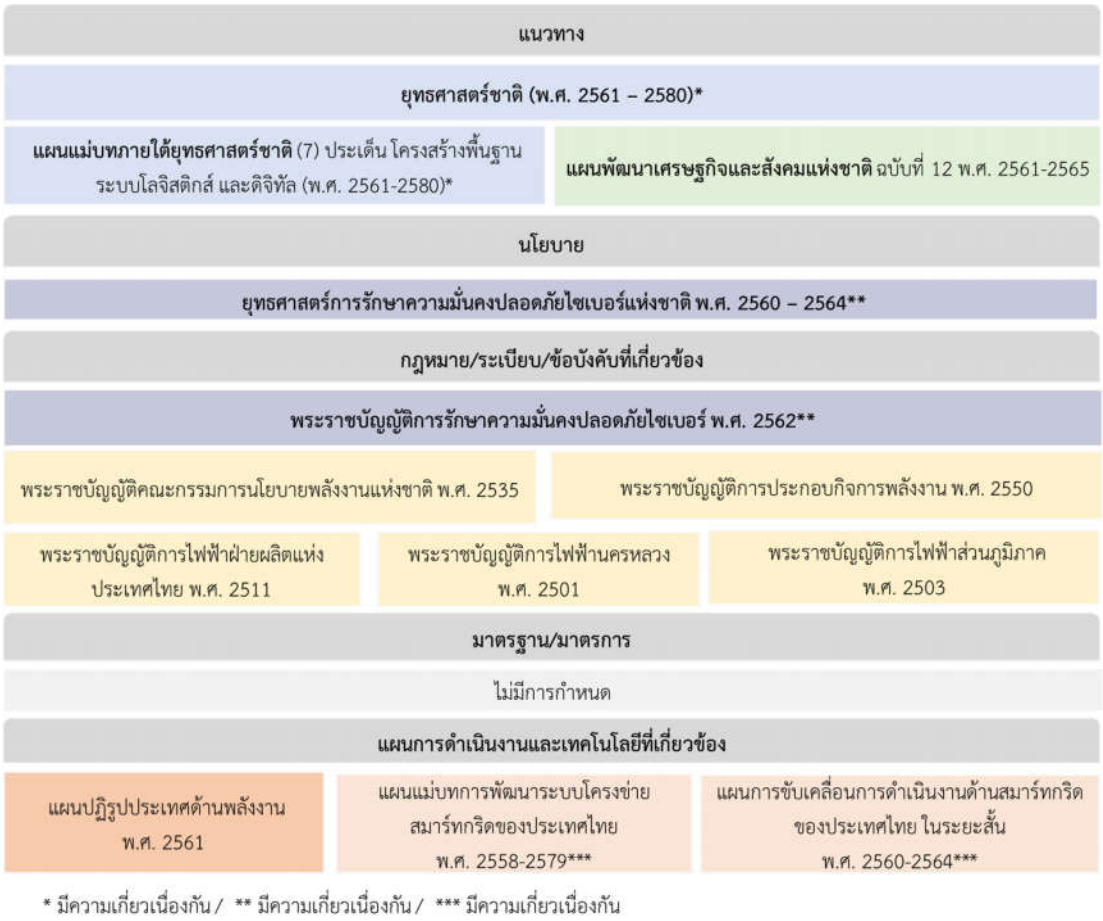


รูปที่ EX-9 ความพร้อมในการรับมือต่อความเสี่ยงด้านไซเบอร์ของภาคส่วนไฟฟ้า

การศึกษาและวิเคราะห์นโยบาย กฎหมาย ระเบียบข้อบังคับที่เกี่ยวข้อง และข้อเสนอแนะ[11]

ที่ปรึกษาได้ดำเนินการศึกษาและวิเคราะห์นโยบาย กฎหมาย ระเบียบข้อบังคับที่เกี่ยวข้อง โดยรวบรวมนโยบาย กฎหมาย ระเบียบข้อบังคับที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยและที่เกี่ยวข้องกับภาคไฟฟ้า ดังปรากฏในรูปที่ EX-10 ซึ่งเป็นการสรุปแนวทางฯ ในการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย ซึ่งจะแบ่งออกได้เป็น 5 ส่วน ได้แก่ (1) แนวทาง (2) นโยบาย (3) กฎหมาย (4) มาตรฐานระเบียบ การกำหนดมาตรการ (5) แผนการดำเนินงาน และเทคโนโลยีที่เกี่ยวข้องในการดำเนินการป้องกันภัยคุกคามทางไซเบอร์

[11] บทที่ 6 การศึกษาและวิเคราะห์นโยบาย กฎหมาย ระเบียบข้อบังคับที่เกี่ยวข้อง และข้อเสนอแนะ



รูปที่ EX-10 แนวทางฯ ในการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย

โดยสรุปบทสรุปผลการวิเคราะห์นโยบาย กฎหมาย ระเบียบข้อบังคับของประเทศไทย ได้ดังนี้

ตารางที่ EX-4 สรุปผลการวิเคราะห์นโยบาย กฎหมาย ระเบียบข้อบังคับของประเทศไทย

นโยบาย กฎหมาย ระเบียบข้อบังคับ	สรุปบทวิเคราะห์
ยุทธศาสตร์และแผนระดับชาติของประเทศไทย	
ยุทธศาสตร์ชาติ (พ.ศ. 2561-2580)	ยุทธศาสตร์ชาติมีการกล่าวถึงยุทธศาสตร์ด้านพลังงานและด้านความมั่นคงปลอดภัยไซเบอร์ หน่วยงานที่เกี่ยวข้องต้องดำเนินงานให้สอดคล้องและเป็นไปในทิศทางเดียวกันกับแผนยุทธศาสตร์ชาติฉบับนี้

นโยบาย กฎหมาย ระเบียบ ข้อบังคับ	สรุปบทวิเคราะห์
แผนแม่บทภายใต้ยุทธศาสตร์ชาติ ((7) ประเด็น โครงสร้างพื้นฐานระบบ โลจิสติกส์ และดิจิทัล) (พ.ศ. 2561-2580)	แผนแม่บทภายใต้ยุทธศาสตร์ชาติมีส่วนที่เกี่ยวข้องกับด้านพลังงานและด้านความมั่นคงปลอดภัยไซเบอร์ ดังต่อไปนี้ **<u>ด้านพลังงาน</u>** มีการกล่าวถึงการพัฒนาในแง่ของระบบโครงข่ายสมาร์ทกริด (Smart Grid) โดยตรง ซึ่งกล่าวได้ว่า อุตสาหกรรมไฟฟ้าในประเทศไทยจะมีแนวโน้มในการนำเทคโนโลยีมาใช้มากขึ้นอย่างชัดเจน จากการส่งเสริมและสนับสนุนในระดับประเทศนี้ **<u>ด้านความมั่นคงปลอดภัยไซเบอร์</u>** ความมั่นคงปลอดภัยทางไซเบอร์ได้รับการพิจารณาเป็นปัจจัยสำคัญปัจจัยหนึ่งสำหรับทางการพัฒนาโครงสร้างพื้นฐานด้านดิจิทัล โดยมีความจำเป็นสำหรับการปกป้องโครงสร้างพื้นฐานของประเทศ รวมถึงโครงสร้างพื้นฐานทางไฟฟ้า ประกอบกับอุตสาหกรรมไฟฟ้าในประเทศไทยจะมีแนวโน้มในการนำเทคโนโลยีสมัยใหม่มาใช้มากขึ้นอย่างชัดเจน ดังนั้น ภาคส่วนไฟฟ้าจึงจำเป็นต้องมีมาตรการเฝ้าระวังและรับมือภัยคุกคามไซเบอร์ที่เหมาะสมและสอดคล้องตามมาตรฐานสากลทั้งในปัจจุบันและในอนาคต
แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 12 พ.ศ. 2561-2565	แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติฉบับที่ 12 มีความเกี่ยวข้องเชื่อมโยงกับด้านพลังงานและด้านความมั่นคงปลอดภัยไซเบอร์ดังต่อไปนี้ **<u>ด้านพลังงาน</u>** มีกล่าวถึงการพัฒนาระบบโครงข่ายสมาร์ทกริด (Smart Grid) ผ่านการส่งเสริมและสนับสนุนการวิจัยและพัฒนาด้านระบบโครงข่ายไฟฟ้าอัจฉริยะให้ครอบคลุมทั้งระบบผลิต ระบบส่ง ระบบจำหน่าย และผู้ใช้ไฟฟ้า เพื่อให้สามารถนำผลการดำเนินการไปใช้ได้จริงในเชิงพาณิชย์ **<u>ด้านความมั่นคงปลอดภัยไซเบอร์</u>** กล่าวถึงการพัฒนาเศรษฐกิจดิจิทัลโดยครอบคลุมถึงการสร้างความมั่นคงปลอดภัยทางไซเบอร์ มีการกล่าวถึงการจัดตั้งศูนย์การเฝ้าระวังและรับมือภัยคุกคามทางไซเบอร์เพื่อดูแลปัญหาและรับมือกับภัยคุกคามที่เปลี่ยนแปลงไปตามความก้าวหน้าของเทคโนโลยี
นโยบาย กฎหมาย ระเบียบข้อบังคับด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย	

นโยบาย กฎหมาย ระเบียบ ข้อบังคับ	สรุปบทวิเคราะห์
ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2660 – 2564 (National Cybersecurity Strategy 2017 – 2021)	**ประเด็นยุทธศาสตร์ที่ 2** มีการกล่าวถึงการจัดทำกรอบนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) โดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นหน่วยงานที่รับผิดชอบหลักในเรื่องดังกล่าว ส่วนหน่วยงานกำกับดูแลโครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นหน่วยงานที่รับผิดชอบลำดับรอง ซึ่งในส่วนนี้ครอบคลุมถึงกระทรวงพลังงานด้วย ดังนั้น ภาคพลังงานจึงจำเป็นต้องมีส่วนร่วมในการกำหนดกรอบนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562	**มาตรา 49** กำหนดให้ภาคส่วนไฟฟ้าจัดเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ด้านพลังงานและสาธารณูปโภคที่มีการประยุกต์ใช้เครือข่ายคอมพิวเตอร์อินเทอร์เน็ต และโครงข่ายโทรคมนาคมในการให้บริการ ซึ่งมีความเสี่ยงจากภัยคุกคามทางไซเบอร์ ภาคส่วนไฟฟ้าจึงต้องมีการดำเนินการเพื่อให้สามารถป้องกันหรือรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที โดยจำเป็นต้องดำเนินการ ดังนี้ (1) กำหนด**หน่วยงานกำกับดูแล**สำหรับภาคส่วนไฟฟ้า และบทบาทหน้าที่ที่ชัดเจน (2) กำหนด**หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ**ในภาคส่วนไฟฟ้า และบทบาทหน้าที่ที่ชัดเจน
แผนการพัฒนาด้านพลังงานไฟฟ้าและสมาร์ทกริดของประเทศไทย	
แผนปฏิรูปประเทศด้านพลังงาน พ.ศ. 2561	แผนปฏิรูปประเทศด้านพลังงาน พ.ศ. 2561 เป็นการกำหนดแผนด้านพลังงานของประเทศปัจจุบันและแนวโน้มในอนาคต 20 ปี การพัฒนาด้านไฟฟ้าเป็น 1 ใน 6 ด้านที่ได้มีการกำหนดแนวทางและแผนไว้อย่างชัดเจน วัตถุประสงค์สำคัญคือเพื่อให้กิจการไฟฟ้าของประเทศไทยมีความมั่นคงปลอดภัย ระบบไฟฟ้าสามารถรองรับการเติบโตทางเศรษฐกิจได้ อย่างไรก็ตาม แผนปฏิรูปฯ ไม่ได้กล่าวถึงการพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์สำหรับระบบไฟฟ้าและระบบสมาร์ทกริดโดยเฉพาะ

นโยบาย กฎหมาย ระเบียบ ข้อบังคับ	สรุปบทวิเคราะห์
แผนแม่บทการพัฒนาระบบโครงข่ายสมาร์ทกริดของประเทศไทย (พ.ศ. 2558-2579)	แผนแม่บทการพัฒนาระบบโครงข่ายสมาร์ทกริดของประเทศไทย (พ.ศ. 2558-2579) กำหนดกรอบทิศทางการพัฒนานโยบายระบบโครงข่ายสมาร์ทกริดของประเทศในภาพรวม โดยให้ความสำคัญกับการพัฒนาและการลงทุนด้านเทคโนโลยี แต่ไม่ได้กล่าวถึงการพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์สำหรับระบบไฟฟ้าและระบบสมาร์ทกริดโดยเฉพาะ
แผนการขับเคลื่อนการดำเนินงานด้านสมาร์ทกริดของประเทศไทยในระยะสั้น (พ.ศ. 2560-2564)	แผนขับเคลื่อนฯ ได้รับการจัดทำขึ้นโดยมีความสอดคล้องกับแผนแม่บทฯ โดยมุ่งเน้นไปที่การขับเคลื่อนหัวข้อด้านสมาร์ทกริดผ่าน 3 เสาหลัก นอกจากนี้ มีการกำหนดแผนสนับสนุนเพิ่มเติมด้าน**การบริหารการขับเคลื่อนฯ และการเตรียมโครงสร้างพื้นฐานที่จำเป็น** ซึ่งในส่วนดังกล่าวพบว่ามีการกล่าวถึงการพัฒนาในแง่ของความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) ของระบบโครงข่ายสมาร์ทกริดโดยตรง โดยมีวัตถุประสงค์เพื่อให้การดำเนินงานด้านสมาร์ทกริดของประเทศไทยมีความมั่นคงปลอดภัยจากภัยคุกคามทางไซเบอร์ต่าง ๆ ทั้งนี้ เนื่องจากการพัฒนาด้านเทคโนโลยีการสื่อสารข้อมูลและทำธุรกรรมทางอิเล็กทรอนิกส์ในโครงข่ายสมาร์ทกริด โดยเฉพาะในเรื่องการดำเนินการตอบสนองด้านโหลด (Demand response: DR) อาจมีการเชื่อมต่อข้อมูลระหว่างผู้รวบรวมโหลด (Load Aggregator: LA) และผู้ใช้ไฟฟ้าผ่านโครงข่ายสาธารณะ ซึ่งเป็นโครงข่ายขนาดใหญ่และมีความเสี่ยงต่อการคุกคามทางไซเบอร์สูง
กฎหมายที่เกี่ยวข้องกับการกำกับดูแลด้านพลังงานของประเทศไทย	

นโยบาย กฎหมาย ระเบียบ ข้อบังคับ	สรุปบทวิเคราะห์
พระราชบัญญัติคณะกรรมการนโยบายพลังงานแห่งชาติ พ.ศ. 2535	พ.ร.บ. คณะกรรมการนโยบายพลังงานแห่งชาติ พ.ศ. 2535 กำหนดให้มีการจัดตั้งคณะกรรมการนโยบายพลังงานแห่งชาติ (กพช.) เพื่อทำหน้าที่ในการพิจารณาเสนอนโยบายและแผนการบริหารและพัฒนาพลังงาน และเนื่องจากการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นประเด็นที่ได้ถูกกล่าวถึงในภายหลัง พ.ร.บ ดังกล่าว จึงไม่ได้มีการระบุถึงบทบาทหน้าที่ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยตรง อย่างไรก็ตาม การนำเอาเทคโนโลยีและการสื่อสารมาใช้งานในภาคพลังงานปัจจุบัน ได้ส่งผลต่อการบริหารและพัฒนาพลังงานของประเทศไทยในปัจจุบันและในอนาคต กพช. จึงจำเป็นต้องพิจารณาด้านนโยบายและแผนการดำเนินงานด้านพลังงาน โดยคำนึงถึงประเด็นด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และดำเนินการให้สอดคล้องกับ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
พระราชบัญญัติการประกอบกิจการพลังงาน พ.ศ. 2550	พ.ร.บ. การประกอบกิจการพลังงาน พ.ศ. 2550 กำหนดให้คณะกรรมการกำกับกิจการพลังงาน (กกพ.) มีบทบาทหน้าที่ในการกำกับดูแลการประกอบกิจการพลังงานซึ่งครอบคลุมถึงผู้รับใบอนุญาตในการประกอบกิจการไฟฟ้า โดยเมื่อพิจารณาจาก พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ประกอบแล้ว จึงกล่าวได้ว่า กกพ. มีอำนาจหน้าที่โดยตรงในการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ของผู้รับใบอนุญาตในการประกอบกิจการไฟฟ้า
พระราชบัญญัติการไฟฟ้าฝ่ายผลิตแห่งประเทศไทย พ.ศ. 2511	พ.ร.บ. การไฟฟ้าฝ่ายผลิตแห่งประเทศไทย พ.ศ. 2511 ได้กล่าวถึงอำนาจหน้าที่และภารกิจ สำหรับการไฟฟ้าฝ่ายผลิตแห่งประเทศไทย (กฟผ.) ในการผลิต จัดหา จัดส่ง หรือจำหน่ายพลังงานไฟฟ้าสำหรับประเทศไทย และเนื่องจากการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นประเด็นที่ได้ถูกกล่าวถึงในภายหลัง พ.ร.บ ดังกล่าว จึงไม่ได้มีการระบุถึงการดำเนินการในด้านนี้ อย่างไรก็ตาม กฟผ. อาจถูกกำหนดเป็นหน่วยงานโครงสร้างพื้นฐานทางสารสนเทศสำคัญด้านพลังงาน เนื่องจากมีการดำเนินภารกิจหลักที่เกี่ยวข้องกับความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ

นโยบาย กฎหมาย ระเบียบ ข้อบังคับ	สรุปบทวิเคราะห์
พระราชบัญญัติการไฟฟ้านครหลวง พ.ศ. 2501	พ.ร.บ. การไฟฟ้านครหลวง พ.ศ. 2501 ได้กล่าวถึงอำนาจหน้าที่และภารกิจ สำหรับการไฟฟ้านครหลวง (กฟน.) ในการผลิต จัดส่ง หรือจำหน่ายพลังงานไฟฟ้าสำหรับกรุงเทพมหานครและปริมณฑล และเนื่องจากการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นประเด็นที่ได้ถูกกล่าวถึงในภายหลัง พ.ร.บ ดังกล่าว จึงไม่ได้มีการระบุถึงการดำเนินการในด้านนี้ อย่างไรก็ตาม กฟน. อาจถูกกำหนดเป็นหน่วยงานโครงสร้างพื้นฐานทางสารสนเทศสำคัญด้านพลังงาน เนื่องจากมีการดำเนินภารกิจหลักที่เกี่ยวข้องกับความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ
พระราชบัญญัติ การไฟฟ้าส่วนภูมิภาค พ.ศ.2503	พ.ร.บ. การไฟฟ้าส่วนภูมิภาค พ.ศ. 2503 ได้กล่าวถึงอำนาจหน้าที่และภารกิจ สำหรับการไฟฟ้าส่วนภูมิภาค (กฟภ.) ในการผลิต จัดส่ง หรือจำหน่ายพลังงานไฟฟ้าสำหรับส่วนภูมิภาคและประเทศใกล้เคียง และเนื่องจากการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นประเด็นที่ได้ถูกกล่าวถึงในภายหลัง พ.ร.บ ดังกล่าว จึงไม่ได้มีการระบุถึงการดำเนินการในด้านนี้ อย่างไรก็ตาม กฟภ. อาจถูกกำหนดเป็นหน่วยงานโครงสร้างพื้นฐานทางสารสนเทศสำคัญด้านพลังงาน เนื่องจากมีการดำเนินภารกิจหลักที่เกี่ยวข้องกับความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ
ระเบียบข้อบังคับ (ด้านความมั่นคงปลอดภัยไซเบอร์)	
-	ปัจจุบัน ยังไม่มีการกำหนดระเบียบ ข้อบังคับด้านความมั่นคงปลอดภัยไซเบอร์ ทั้งในระดับประเทศ และภาคส่วนไฟฟ้า ในขณะที่ทำการศึกษาหัวข้อนี้

โดยจากการศึกษาข้อมูลตามนโยบาย กฎหมาย ระเบียบข้อบังคับที่กล่าวมาพบว่าภาคไฟฟ้ามีความจำเป็นต้องดำเนินการบางส่วนเพื่อปกป้องและ/หรือป้องกันภัยคุกคามทางไซเบอร์สำหรับระบบไฟฟ้าของประเทศไทยในปัจจุบันและในอนาคตในส่วนงานด้านสมาร์ทกริด โดยจะต้องสอดคล้องกับแนวทางและกฎหมายการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ โดยประเด็นที่เสนอแนะสามารถสรุปได้ดังรูปที่ EX-5

ตารางที่ EX-5 แนวทางการดำเนินงานเพื่อปกป้องและ/หรือป้องกันภัยคุกคามทางไซเบอร์สำหรับระบบไฟฟ้าของประเทศ

ลำดับ	หัวข้อหลัก	หัวข้อย่อย
1	การบริหารจัดการเชิงนโยบาย	■ กำหนดนโยบายการบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ■ เข้าร่วมการรับฟังความเห็นหรือประชุมในการจัดทำนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ร่วมกับสำนักงาน กมช. ■ กำหนดมาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญ
2	กำหนดโครงสร้างการบริหารจัดการด้านไซเบอร์ของภาคส่วนไฟฟ้า	■ มอบหมายการควบคุมและกำกับดูแล รวมถึงการออกข้อกำหนด วัตถุประสงค์ หน้าที่และอำนาจ และกรอบการดำเนินการ ■ ร่วมกำหนดลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์
3	กำหนดขอบเขตการกำกับดูแลด้านไซเบอร์ของภาคส่วนไฟฟ้า	■ ประกาศกำหนดลักษณะหน่วยงานที่มีภารกิจหรือให้บริการในด้านที่กำหนด เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
4	กำหนดแนวทางในการปฏิบัติเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ของภาคส่วนไฟฟ้า	■ กำหนดมาตรฐานขั้นต่ำ ■ กำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์/แผนการรับมือภัยคุกคามทางไซเบอร์ / กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์)

ทั้งนี้ การดำเนินการด้านต่าง ๆ จำเป็นต้องดำเนินการภายในช่วงเวลาที่เหมาะสมและมีความสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับต่าง ๆ รวมถึงแผนที่เกี่ยวข้องกับการพัฒนาระบบไฟฟ้าและสมาร์ทกริดของประเทศไทย ซึ่งจะครอบคลุมช่วงปี 2563 – 2579 โดยประกอบด้วยแผนระยะสั้น แผนระยะปานกลาง และแผนระยะยาว (ดังปรากฏในรูปที่ EX-11)

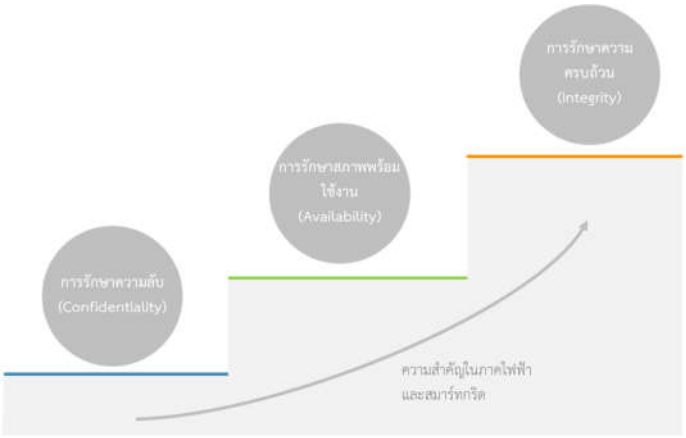
รูปที่ EX-11 แผนในการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย

กรอบ ขอบเขต และแนวทางการรักษาความปลอดภัยด้านไซเบอร์สำหรับระบบไฟฟ้าของไทย[12]

ภาคส่วนไฟฟ้าถือเป็นโครงสร้างพื้นฐานที่สำคัญของประเทศ (Critical Infrastructure: CI) หน่วยงานที่เกี่ยวข้องในภาคไฟฟ้าจึงมีความจำเป็นต้องปกป้องระบบไฟฟ้าให้มีเสถียรภาพ และพร้อมให้บริการอยู่เสมอ ด้วยแนวโน้มของเทคโนโลยี และการสื่อสารที่เปลี่ยนแปลงไป จึงต้องคำนึงถึงภัยคุกคามทางไซเบอร์และให้ความสนใจมากขึ้นเนื่องจากอาจก่อให้เกิดเหตุการณ์ไฟฟ้าดับเป็นวงกว้าง จนอาจกลายเป็นเหตุวิกฤติที่จะส่งผลกระทบระดับประเทศได้

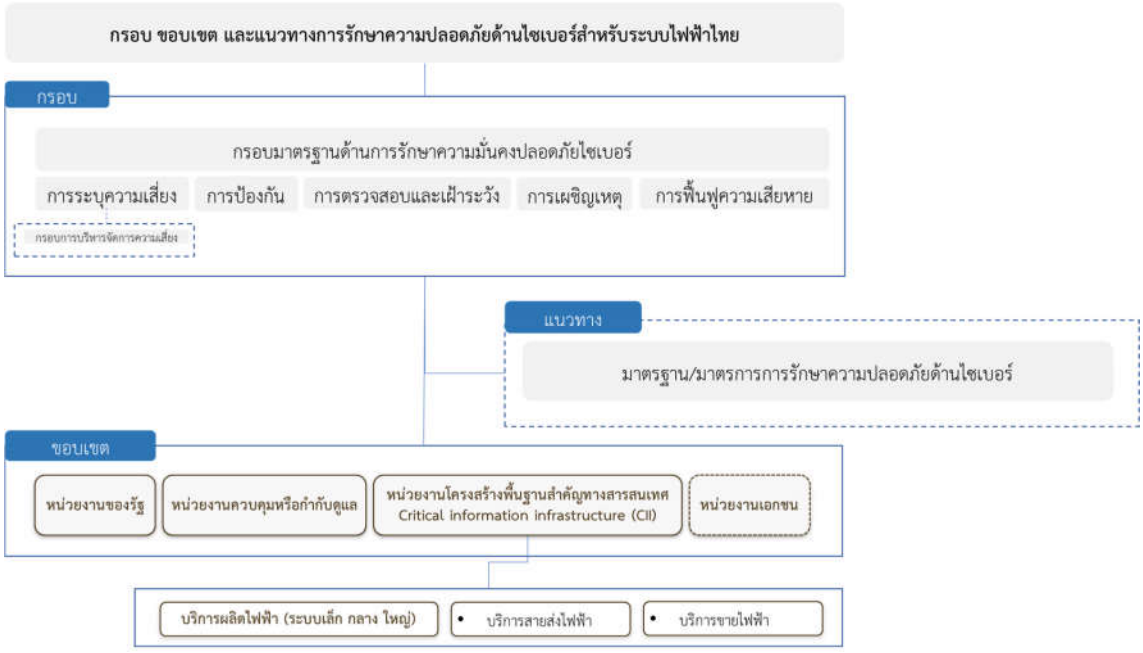
ดังนั้น จึงจำเป็นต้องมีการกำหนด**กรอบ ขอบเขต และแนวทางการรักษาความปลอดภัยด้านไซเบอร์** เพื่อกำกับดูแลให้ผู้ประกอบกิจการไฟฟ้าสามารถรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับระบบไฟฟ้า และระบบสมาร์ทกริดที่สอดคล้องกับวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ 3 ประการซึ่งได้แก่ การรักษาความลับ (Confidentiality) การรักษาความครบถ้วน (Integrity) และการรักษาสภาพพร้อมใช้งาน (Availability) (ดังปรากฏในรูปที่ EX-12) รวมถึงสอดคล้องกับแนวทาง กฎหมาย ระเบียบข้อบังคับของประเทศ

[12] บทที่ 5 กรอบขอบเขตและแนวทางการรักษาความปลอดภัยด้านไซเบอร์สำหรับระบบไฟฟ้าของไทย



รูปที่ EX-12 วัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับระบบไฟฟ้าและสมาร์ทกริด

ปัจจุบัน ประเทศไทยยังไม่มีการกำหนดกรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศโดยหน่วยงานใดหน่วยงานหนึ่ง มีเพียง**พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562** ซึ่งบังคับใช้กับหน่วยงานโครงสร้างพื้นฐานที่สำคัญ (Critical Infrastructure: CI) ซึ่งด้านพลังงานและสาธารณูปโภครวมอยู่ใน CI ด้วย ทั้งนี้ ภาคส่วนไฟฟ้าอาจพิจารณาเพิ่มเติม ในการกำหนด กรอบการบริหารจัดการความเสี่ยงด้านภัยคุกคามไซเบอร์ ซึ่งจะช่วยให้การดำเนินงานด้านการประเมินความเสี่ยงสำหรับภาคส่วนไฟฟ้าเป็นไปในทิศทางเดียวกัน (ดังปรากฏในรูปที่ EX-13)



รูปที่ EX-13 ภาพรวมการกำหนดกรอบ ขอบเขตและแนวทางการรักษาความปลอดภัยด้านไซเบอร์สำหรับระบบไฟฟ้าของไทย

เพื่อให้กรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ของภาคส่วนไฟฟ้า ให้มีความสอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 หน่วยงานภาคนโยบายจำเป็นต้องกำหนดกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยต้องครอบคลุมถึง 5 องค์ประกอบหลัก

- การระบุความเสี่ยง (Identify) ที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ระบบคอมพิวเตอร์ข้อมูลคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ รวมไปถึงความเสี่ยงต่อชีวิตและทรัพย์สิน
- มาตรการป้องกันความเสี่ยง (Protect) ซึ่งครอบคลุมถึง การรักษาความลับ (Confidentiality) การรักษาความครบถ้วน (Integrity) และการรักษาสภาพความพร้อมใช้งาน (Availability) เป็นขั้นต่ำ
- มาตรการตรวจสอบและเฝ้าระวัง (Detect) ภัยคุกคามทางไซเบอร์
- มาตรการเผชิญเหตุ (Response) เมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์
- มาตรการรักษาและฟื้นฟูความเสียหาย (Recover) ที่เกิดจากภัยคุกคามทางไซเบอร์

เนื่องด้วยแนวทางในการบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์ที่ต้องมีความสอดคล้องกับกรอบการบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์นั้น ซึ่งได้แก่ มาตรฐาน หรือมาตรการการรักษาความปลอดภัยด้านไซเบอร์ที่ถือว่าเป็นมาตรฐานขั้นต่ำหรือที่จำเป็น อาจไม่ได้มีการระบุถึงรายละเอียดไว้ในเนื้อหาของกฎหมาย อย่างไรก็ตาม ได้มีข้อเสนอแนะ[13] รวมถึงจากการหารือร่วมกับระหว่างหน่วยงานการไฟฟ้า และภาคเอกชนในปัจจุบัน พบว่า การไฟฟ้าและภาคเอกชนได้มีการกำหนดแนวทางการรักษาความปลอดภัยด้านไซเบอร์เบื้องต้นสำหรับระบบไฟฟ้าของตนเองไว้แล้ว โดยพิจารณาจากความเสี่ยงและได้กำหนดมาตรการป้องกันตามความเหมาะสมซึ่งประกอบด้วยมาตรฐาน **ISO/IEC 27001** และมาตรการตาม **NERC CIP**

ทั้งนี้ จากการวิเคราะห์ความสอดคล้องกับแนวทางตามกรอบของ **NIST CSF** และ**พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562** พบว่ามาตรฐาน/มาตรการดังกล่าว สามารถนำมาใช้เป็นแนวทางการรักษาความปลอดภัยด้านไซเบอร์สำหรับระบบไฟฟ้าของไทยได้

นอกจากนี้ เพื่อให้การดำเนินงานด้านการปกป้องความเสี่ยงจากภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ กรอบการบริหารจัดการความเสี่ยงความมั่นคงปลอดภัยไซเบอร์จำเป็นต้องถูกกำหนดขึ้นเพื่อใช้เป็นกรอบปฏิบัติสำหรับการดำเนินการตามมาตรการการระบุความเสี่ยงที่เป็นมาตรฐานเดียวกันทั้งภาคส่วนไฟฟ้า ทั้งนี้ กรอบฯ ดังกล่าวจะช่วยให้องค์กรสามารถวิเคราะห์ความเสี่ยง และบริหารจัดการความเสี่ยงขององค์กรได้อย่างมีประสิทธิภาพและมีประสิทธิผล

[13] อ้างอิงจากเอกสารประกอบการประชุมหารือแนวทางกำหนดหลักเกณฑ์บริการที่สำคัญของ CII เดือนมีนาคม พ.ศ.2563 กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ปัจจุบัน ยังไม่มีการกำหนดกรอบการบริหารจัดการความเสี่ยงความมั่นคงปลอดภัยไซเบอร์ในระดับประเทศหรือในระดับภาคส่วนพลังงานที่ชัดเจน โดยจากการหารือร่วมกันระหว่างหน่วยงานการไฟฟ้าและภาคเอกชนในปัจจุบัน พบว่าได้มีการกำหนดกรอบในการบริหารจัดการความเสี่ยงความมั่นคงปลอดภัยไซเบอร์โดยอ้างถึงมาตรฐานสากล ยกตัวอย่างเช่น NIST800-30 ISO/IEC27005 และ ISO31000 เป็นต้น ซึ่งหน่วยงานภาคนโยบายสามารถพิจารณาผลการดำเนินการตามกรอบฯ ดังกล่าว โดยไม่จำเป็นต้องมีการกำหนดกรอบในการบริหารจัดการความเสี่ยงความมั่นคงปลอดภัยไซเบอร์เพิ่มเติม

ข้อเสนอแนะโครงสร้างการบริหารจัดการทั้งในระยะสั้นและระยะยาว รวมถึงบทบาทหน้าที่ [14]

การดำเนินการภายใต้กรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์เพื่อรองรับการขับเคลื่อนการพัฒนาที่อาจเกิดขึ้นในอนาคต ควรต้องมีการเตรียมการต่าง ๆ ทั้งในด้านการกำหนดโครงสร้างหน่วยงาน การกำหนดบทบาทหน้าที่ในการดำเนินมาตรการต่าง ๆ ทางด้านความมั่นคงปลอดภัยไซเบอร์ไว้ โดยจำแนกโครงสร้างและบทบาทหน้าที่ออกเป็นสองกลุ่มด้วยกัน ได้แก่

(1) การดำเนินการด้านการควบคุมหรือกำกับดูแล

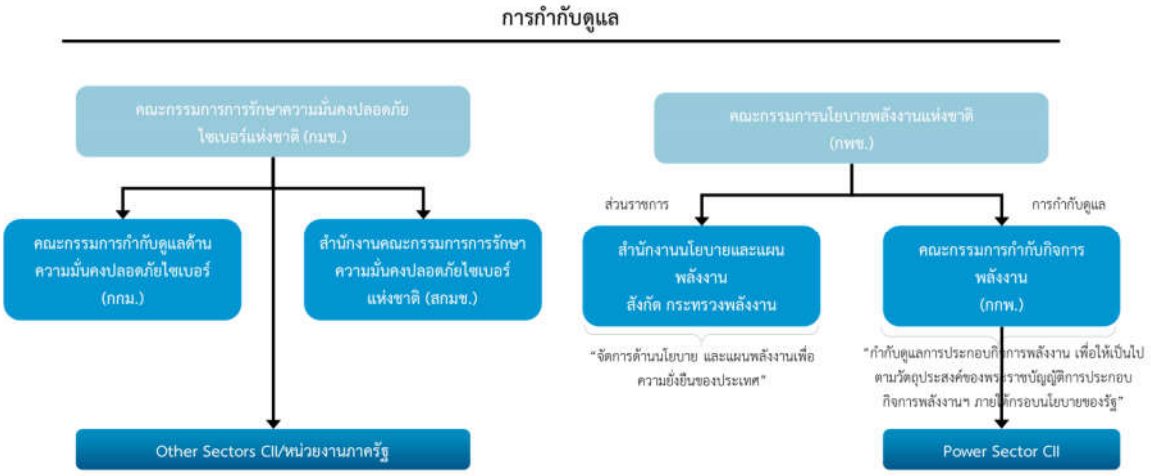
จากบริบทของกิจการพลังงานไฟฟ้าในปัจจุบัน หน่วยงานที่เข้าข่ายเป็นหน่วยงานควบคุมหรือกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา 49 (6) ด้านพลังงานและสาธารณูปโภค เฉพาะที่เกี่ยวข้องกับด้านพลังงานไฟฟ้า ของ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ได้แก่ **คณะกรรมการกำกับกิจการพลังงาน (กกพ.)** ซึ่งได้รับการแต่งตั้งขึ้นเป็นองค์กรกลางในการกำกับดูแลกิจการพลังงานของประเทศ ตามพระราชบัญญัติการประกอบกิจการพลังงาน พ.ศ. 2550 ทำหน้าที่กำกับดูแลผู้รับใบอนุญาตประกอบกิจการพลังงาน ซึ่งครอบคลุมถึงการไฟฟ้าทั้ง 3 แห่ง และผู้ประกอบกิจการพลังงานภาคเอกชน

อย่างไรก็ตาม การดำเนินงานด้านการควบคุมหรือกำกับดูแล ด้านความมั่นคงปลอดภัยทางไซเบอร์ อาจมิได้ถูกกำหนดหรือมอบหมายโดยตรงจากกฎหมายที่เกี่ยวข้องกับการประกอบกิจการพลังงาน หรือ พ.ร.บ. การไฟฟ้า อย่างไรก็ดี หน่วยงานควบคุมหรือกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จะสามารถดำเนินการกำหนดมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ เช่น การเข้าตรวจสอบ การสั่งการให้แก้ไข หรือดำเนินการอย่างหนึ่งอย่างใด เป็นต้น ทั้งนี้ โดยอาศัยอำนาจของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) เพื่อลดขั้นตอนการแก้กฎหมายของกิจการพลังงานโดยตรงได้

ทั้งนี้ ในอนาคต ควรพิจารณาสร้างความร่วมมือกันระหว่างคณะกรรมการกำกับกิจการพลังงาน (กกพ.) และกระทรวงมหาดไทย เนื่องด้วยการวางนโยบายและควบคุมดูแลกิจการของการไฟฟ้านครหลวงและการไฟฟ้าภูมิภาค ซึ่งเป็นหน่วยงานภาครัฐวิสาหกิจขนาดใหญ่ ได้อยู่ภายใต้การกำกับดูแลของ

[14] บทที่ 7 ข้อเสนอแนะโครงสร้างการบริหารจัดการทั้งในระยะสั้นและระยะยาว รวมถึงบทบาทหน้าที่

กระทรวงมหาดไทย เพื่อให้เกิดการดำเนินงานการกำกับดูแลด้านความมั่นคงปลอดภัยทางไซเบอร์แบบศูนย์กลางและเป็นมาตรฐานเดียวกัน



รูปที่ EX-14 โครงสร้างการกำกับดูแลภาคส่วนไฟฟ้า

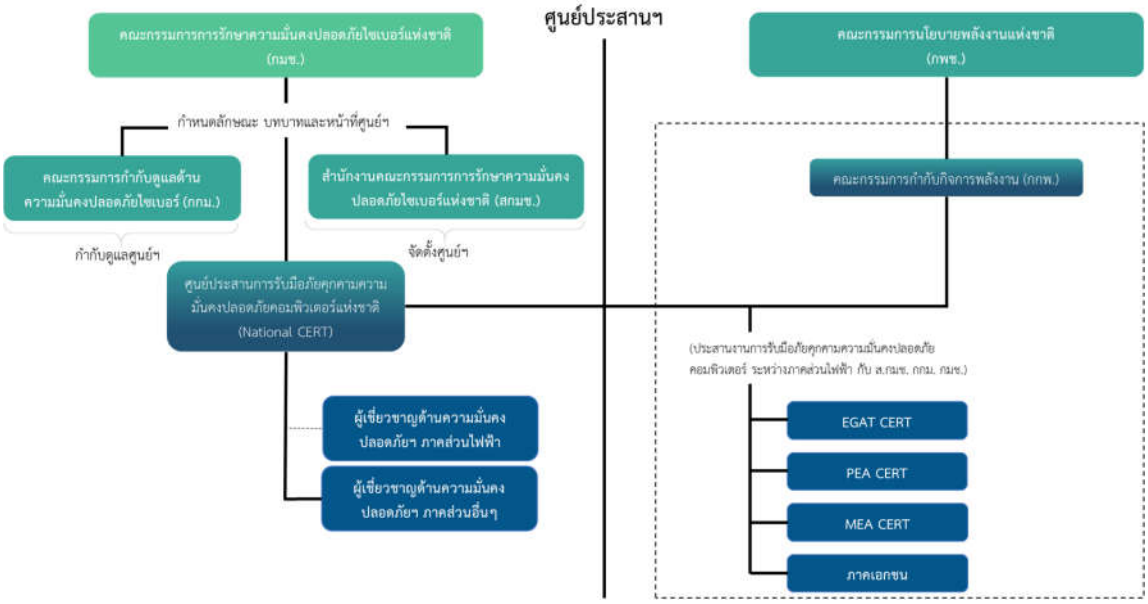
(2) การดำเนินการด้านศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์

จากบริบทของกิจการพลังงานไฟฟ้าในปัจจุบัน ไม่พบว่ามีการดำเนินงานด้านศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับภาคส่วนไฟฟ้าโดยเฉพาะ เพื่อทำหน้าที่ในการประสานงาน เฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์ อย่างไรก็ตาม พบว่าได้มีการดำเนินงานบางส่วนในหน่วยงานภาครัฐวิสาหกิจและเอกชนขนาดใหญ่

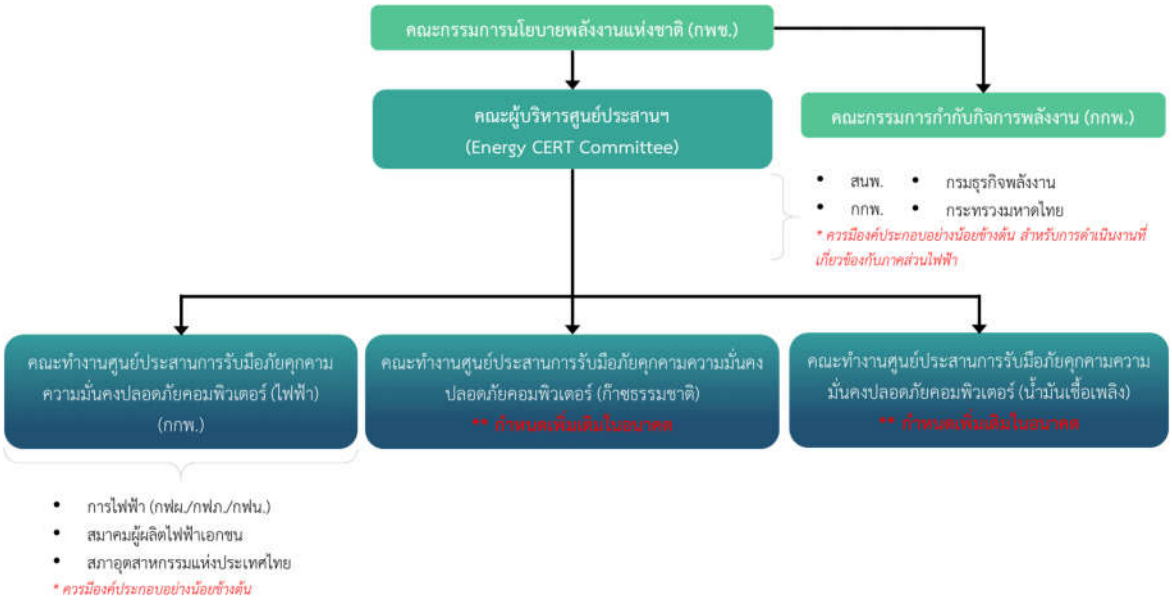
เนื่องจากภารกิจดังกล่าวเป็นเรื่องใหม่ที่ภาคส่วนไฟฟ้ายังไม่มีความคุ้นเคยในการดำเนินงาน รวมถึงมีความจำเป็นที่ต้องลงทุนด้านเทคโนโลยีและการพัฒนาบุคลากร และอาศัยระยะเวลาในการพัฒนา ซึ่งไม่สามารถดำเนินการได้ภายในระยะเวลาอันสั้น จึงอาจพิจารณาแบ่งแผนการดำเนินงานออกเป็นสองระยะด้วยกัน ได้แก่ แผนระยะสั้น-กลาง เป็นการดำเนินงานให้มีความสอดคล้องกับกฎหมายด้านไซเบอร์ของประเทศ และแผนระยะกลาง-ยาว เป็นการพิจารณากำหนดหน่วยงานที่รับผิดชอบด้านศูนย์ประสานฯ สำหรับภาคส่วนไฟฟ้าโดยเฉพาะ ประกอบด้วย

แผนระยะสั้น-กลาง พิจารณาแนวทางในการร่วมมือกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ หรือ National Computer Emergency Response (National CERT) โดยให้หน่วยงานโครงสร้างพื้นฐานฯ ภายในภาคส่วนไฟฟ้า ประสานกับ National CERT โดยตรงในกรณีที่ต้องประสานงาน เฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์

แผนระยะกลาง-ยาว ในอนาคต หน่วยงานกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานฯ อาจร่วมพิจารณาตั้งส่วนงานภายในที่รับผิดชอบด้านศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับภาคส่วนไฟฟ้าหรือภาคส่วนพลังงานโดยตรง ซึ่งจะสอดคล้องกับโครงสร้างของหน่วยงานโครงสร้างพื้นฐานฯ ด้านอื่น ๆ เช่น ด้านการเงินการธนาคาร ซึ่งได้มี ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคธนาคาร หรือ Thailand Banking Sector Computer Emergency Response (TB-CERT) ซึ่งมีหน้าที่หลักในการเตรียมพร้อมรับมือกับภัยคุกคามไซเบอร์ทางการเงิน ทั้งนี้ เพื่อให้มีการดำเนินการที่เป็นศูนย์กลางสำหรับหน่วยงานโครงสร้างพื้นฐานด้านพลังงานในภาพรวม ในระยะยาว



รูปที่ EX -15 โครงสร้างการบริหารจัดการด้านศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ในระยะสั้น-กลาง



รูปที่ EX-16 โครงสร้างการบริหารจัดการด้านศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ในระยะกลาง-ยาว

สรุปการจัดประชุมกลุ่มย่อยฯ [15]

ตามที่ข้อกำหนดโครงการฯ ได้กำหนดให้ต้องมีจัดประชุมกลุ่มย่อย เฉพาะรายหน่วยงาน/องค์กร/ผู้มีส่วนได้ส่วนเสีย (ทวิภาคี) หรือหลายหน่วยงาน/องค์กร/ผู้มีส่วนได้ส่วนเสียพร้อมกัน (พหุภาคี) ตามความเหมาะสมจำเป็น เพื่อรับทราบสถานการณ์ปัจจุบัน แลกเปลี่ยนข้อมูล หารือเชิงลึก และระดมสมองเพื่อจัดทำแผนการพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับสมาร์ทกริด จำนวนไม่น้อยกว่า 8 ครั้ง รวมจำนวนผู้เข้าร่วมไม่น้อยกว่า 240 ท่าน

โดยปัจจุบันมีสถานะการดำเนินการระหว่างวันที่ 12 กรกฎาคม พ.ศ. 2562 – 11 กันยายน พ.ศ. 2563 แบ่งเป็น 2 ระยะ ดังนี้

1. สรุปการประชุมและจำนวนผู้เข้าร่วมประชุม ประกอบผลการดำเนินงานฉบับที่ 1 (แนบรายงานการประชุมในรายงานผลการดำเนินงานฉบับที่ 1)
   - จำนวนครั้งที่จัดประชุมทั้งหมด 5 ครั้ง
   - จำนวนผู้เข้าร่วมประชุมทั้งหมด 111 ท่าน
2. สรุปการประชุมและจำนวนผู้เข้าร่วมประชุม ประกอบผลการดำเนินงานฉบับที่ 2 (แนบรายงานการประชุมในรายงานฉบับนี้)
   - จำนวนครั้งที่จัดประชุมทั้งหมด 5 ครั้ง
   - จำนวนผู้เข้าร่วมประชุมทั้งหมด 38 ท่าน

[15] บทที่ 7 ข้อเสนอแนะโครงสร้างการบริหารจัดการทั้งในระยะสั้นและระยะยาว รวมถึงบทบาทหน้าที่

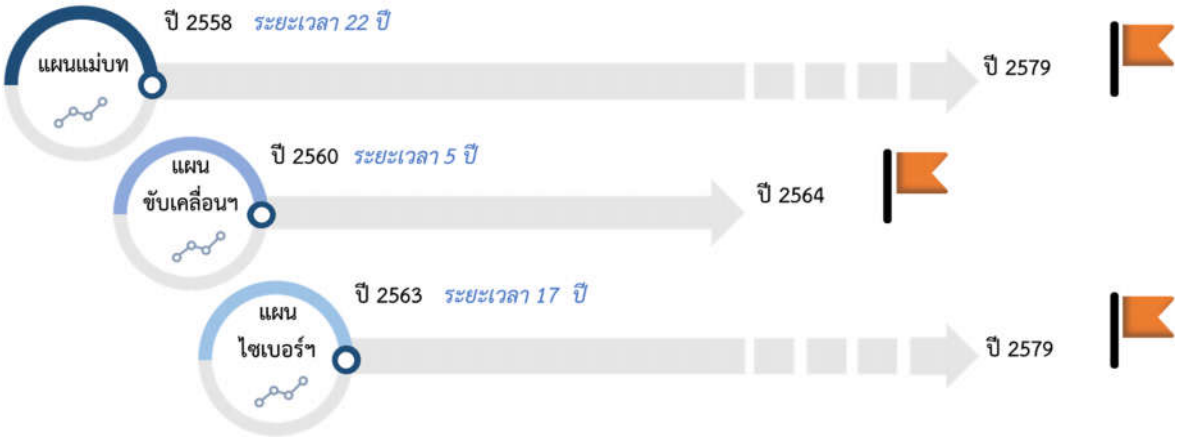
3. สรุปการประชุมและจำนวนผู้เข้าร่วมประชุม ประกอบผลการดำเนินงานฉบับที่ 3 (แนบรายงานการประชุมในรายงานฉบับนี้)

- จำนวนครั้งที่จัดประชุมทั้งหมด 5 ครั้ง
- จำนวนผู้เข้าร่วมประชุมทั้งหมด 142 ท่าน

สรุปจำนวนครั้งที่จัดประชุมทั้งหมด 15 ครั้ง ผู้เข้าร่วมประชุมสะสมทั้งหมด 291 ท่าน

สรุปการจัดทำ(ร่าง) แผนการพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับสมาร์ทกริด

การดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์สำหรับภาคส่วนไฟฟ้านั้น ได้เน้นไปยัง 4 หัวข้อหลักด้วยกัน ได้แก่ การบริหารจัดการเชิงนโยบายและโครงสร้างการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ การพัฒนาศักยภาพและเพิ่มทักษะบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ การกำหนดขอบเขตการกำกับดูแลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของภาคส่วนไฟฟ้า และการกำหนดแนวปฏิบัติเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ของภาคส่วนไฟฟ้า โดยแผนการดำเนินการในแต่ละด้าน จะแบ่งออกเป็นแผนระยะสั้น ระยะกลาง และระยะยาว ซึ่งจะสอดคล้องและเป็นไปตามระยะเวลาของแผนแม่บทการพัฒนาระบบโครงข่ายสมาร์ทกริดของประเทศไทย พ.ศ. 2558-2579 และแผนการขับเคลื่อนการดำเนินงานด้านสมาร์ทกริดของประเทศไทย ในระยะสั้น (พ.ศ. 2560 - 2564) โดยแผนการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2565 – 2579 มีกรอบระยะเวลาครอบคลุม 17 ปี



รูปที่ EX-17 ภาพรวมแผนการพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับสมาร์ทกริด

แผนการพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับสมาร์ทกริดทั้ง 4 กลุ่ม ได้มีการกำหนดข้อเสนอแนะเชิงนโยบาย วัตถุประสงค์และผลลัพธ์ รวมถึงกรอบระยะเวลาดำเนินงาน ดังนี้

- แผนกลุ่มที่ 1 การบริหารจัดการเชิงนโยบาย และโครงสร้างการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของภาคส่วนไฟฟ้า
- แผนกลุ่มที่ 2 การพัฒนาศักยภาพและเพิ่มทักษะบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของภาคส่วนไฟฟ้า
- แผนกลุ่มที่ 3 การกำหนดขอบเขตการกำกับดูแลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของภาคส่วนไฟฟ้า
- แผนกลุ่มที่ 4 การกำหนดแนวปฏิบัติเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ของภาคส่วนไฟฟ้า

สรุปการจัดประชุมผู้มีส่วนได้ส่วนเสีย เพื่อรับฟังความคิดเห็นต่อ “ร่าง” แผนการพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับสมาร์ทกริด

ตามที่ข้อกำหนดโครงการฯ ได้กำหนดให้ต้องมีการจัดประชุมผู้มีส่วนได้ส่วนเสีย เพื่อรับฟังความคิดเห็นต่อ “ร่าง” แผนการพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับสมาร์ทกริด จำนวนอย่างน้อย 1 ครั้ง ผู้เข้าร่วมรวมไม่น้อยกว่า 150 ท่าน

ทั้งนี้ เมื่อวันพุธที่ 4 พฤศจิกายน พ.ศ. 2563 ที่ผ่านมา บริษัทฯ ได้ดำเนินการจัดประชุมสัมมนารับฟังความคิดเห็น ต่อร่างแผนการพัฒนาการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ เรียบร้อยแล้ว โดยสรุปจำนวนผู้เข้าร่วมประชุมทั้งหมด 156 ท่าน ดังนี้

หน่วยงาน	จำนวน
สำนักงานนโยบายและแผนพลังงาน	12
การไฟฟ้าฝ่ายผลิตแห่งประเทศไทย	27
การไฟฟ้าส่วนภูมิภาค	28
การไฟฟ้านครหลวง	26
สำนักงานคณะกรรมการกำกับกิจการพลังงาน	2
สมาคมยานยนต์ไฟฟ้าไทย	1
สมาคมผู้ผลิตไฟฟ้าเอกชน	7
สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.)	3
สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรศัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.)	2
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง	1
กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม	1
กรมธุรกิจพลังงาน	3
กรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน	3
กระทรวงมหาดไทย	2
ธนาคารแห่งประเทศไทย	4
บริษัท กสท โทรคมนาคม จำกัด (มหาชน)	2
บริษัท ไซเบอร์ตรอน จำกัด	2
บริษัท ไทยออยล์ จำกัด	1
บริษัท ทีโอที จำกัด (มหาชน)	1
บริษัท พีทีที ดิจิตอล โซลูชั่น จำกัด	3
บริษัท แอร์โรว์ ไอที ซิสเต็มส์ จำกัด	1
บริษัท อินค็อกนิโคแล็บ จำกัด	2
โรงไฟฟ้าบีแอลซีพี	3
สถาบันเทคโนโลยีไทย-ญี่ปุ่น	3
บริษัท เอส เทลลิเจนซ์ จำกัด	1
สมาคมความมั่นคงปลอดภัยระบบสารสนเทศ	15
รวมทั้งหมด	**156**